# COWLITZ TRIBAL GAMING COMMISSION

## Tribal Internal Control Standards

CTGC-REG-2026-01

Revised May 26, 2026

Adopted by Commission Resolution 2026-01

# Chapter 1 OVERVIEW

## 1.1. Authority

A. The Cowlitz Tribal Gaming Commission, under authority of the Indian Gaming Regulatory Act of 1988, utilizing the National Indian Gaming Commission's Minimum Internal Control Standards (MICS), the 25 CFR Part 542, 543 and 547 regulations as a framework to create regulations to be known as Tribal Internal Control Standards (TICS).

## 1.2. Scope

A. These regulations contain standards and procedures that govern cash handling, documentation, game integrity, auditing, surveillance, information technology, complimentary services or items, gaming promotions and player tracking systems, drop and count, as well as other areas. MICS 542.3(c)

B. Also contained in the TICS are standards for currency transaction reporting in accordance with 31 CFR Part 1021 (Effective March 1, 2011).

## 1.3. Order of Resolution

A. How do these regulations affect the Class III gaming minimum internal control standards established in the Tribal-State Compact? MICS 542.4

1. If there is a direct conflict between the Tribal-State Compact and this document, then the Tribal-State Compact shall prevail.
2. If the Tribal-State Compact provides a level of control that equals or exceeds the level of control under this document, then the Tribal-State Compact standard shall prevail.
3. If this document provides a level of control that exceeds the level of control under the Tribal-State Compact, then this document shall prevail.

# Chapter 2 DEFINITIONS

## 2.1. The following are definitions for terms used in this document.

Accountability means all financial instruments, receivables, and patron deposits constituting the total amount for which the bankroll custodian is responsible at a given time.

Accumulated Credit Payout means credit earned in an Electronic Gaming Machine that is paid to a customer via a cash-out ticket.

Actual Hold Percentage means the percentage calculated by dividing the win by the drop. Can be calculated for individual games or type of games on a per-day or cumulative basis.

Agent (or employee, staff, personnel, team member) means a person authorized by the gaming operation, as approved by the TGA, to make decisions or perform assigned tasks or actions on behalf of the gaming operation.

AICPA means the American Institute of Certified Public Accountants.

Annual means one full calendar year; not to exceed 15 months

Automated payout means payment issued by a machine.

Bank or Bankroll means the inventory of currency, coins, chips, and cash equivalents in the cage, pit area, cashiering locations, and on the playing tables and cash in bank which is used to make change, pay winnings, bets, and pay electronic game jackpots.

Cage means a secure work area within the gaming operation for cashiers, which may include a storage area for the gaming operation bankroll.

Cage Accountability Form or Accountability Form means an itemized list of the components that make up the cage accountability.

Card Games means a game in which the gaming operation is not party to wagers and from which the gaming operation receives compensation in the form of a rake-off, a time buy-in, or other fee or payment from a player for the privilege of playing.

Card Room Bank means the operating fund assigned to the card room or main card room bank.

Cash equivalents means a treasury check, personal check, travelers check, wire transfer of funds, money order, certified check, cashier's check, a check drawn on the Tribal Gaming Operation payable to the patron or to the Tribal Gaming Operation, or a voucher recording cash drawn against a credit card or charge card.

Cashless system means a system that performs cashless transactions and maintains records of those cashless transactions.

Cashless transaction means a movement of funds electronically from one component to another.

Cash-Out Ticket means an instrument of value generated by an EGM representing a monetary amount owed to a customer at a specific electronic gaming machine. This investment may be wagered at other machines by depositing the cash-out ticket in the machine document acceptor.

Chair of NIGC means the Chair of the National Indian Gaming Commission.

Chip means a money substitute, in various denominations, issued by a gaming establishment and used for wagering.

Chip Tray means that container located on gaming tables where chips are stored that are used in the game.

Class II gaming means Class II gaming has the same meaning as defined in 25 U.S.C. 2703(7)(A).

Class III gaming means gaming that is govern by the Tribal-State Compact

Class II gaming system means all components, whether or not technologic aids in electronic, computer, mechanical, or other technologic form, that function together to aid the play of one or more Class II games, including accounting functions mandated by these regulations or part 547 of this chapter.

Complimentary services and items (or Comps) means services and items provided to a patron at the discretion of an agent on behalf of the gaming operation or by a third party on behalf of the gaming operation. Services and items may include, but are not limited to, travel, lodging, food, non-alcoholic beverages, or entertainment expenses.

Count means the act of counting and recording the drop and/or other funds. Also, the total funds counted for a particular game, player interface, shift, or other period.

Count room means a secured room where the count is performed in which the cash and cash equivalents are counted.

Coupon means a financial instrument of fixed wagering value that can only be used to acquire non-cashable credits through interaction with a voucher system. This does not include instruments such as printed advertising material that cannot be validated directly by a voucher system.

CPA means Certified Public Accountant. Professional accountant(s) who is qualified and sufficiently independent to act as auditor of the tribal gaming operations.

Credit-In Meter means a meter that records the amount wagered as a result of credits played.

Credit Slip means a form used to record the return of chips from a gaming table to the cage.

CTGC means the Cowlitz Tribal Gaming Commission.

Currency cassette means a compartment that contains a specified denomination of currency. Currency cassettes are inserted into kiosks, allowing them to dispense currency.

Dealer/Boxperson means an employee who operates a game, individually or as a part of a crew, administering house rules and making payoffs.

Dedicated camera means a video camera that continuously records a specific activity.

Download package means approved data sent to a component of a gaming system for such purposes as changing the component software.

Drop means the total amount of cash and/or cash equivalent removed from the drop box.

Drop Box means a locked container attached to a gaming station, EGM or remote point of sales in which cash or cash equivalents are placed at the time of a transaction.

Drop Box Cabinet means the wooden or metal base of the gaming machine that contains the gaming machine drop box.

Drop Box Contents Key means the key used to open drop boxes.

Drop Box Release Key means the key used to release drop boxes from gaming station or EGM.

Drop Box Storage Rack Key means the key used to access the storage rack where drop boxes are secured.

Drop period means the period of time that occurs between sequential drops.

Drop Proceeds means the total amount of financial instruments removed from drop boxes and financial instrument storage components.

Electronic Gaming Machine or EGM means an electronic or electromechanical device that allows a player to play games of chance. Such device is activated by the insertion of a ticket, currency or credit purchased currency and awards game credits or a written statement of the player's accumulated credits, which written statements are redeemable for cash.

Electromagnetic interference means the disruption of operation of an electronic device when it is in the vicinity of an electromagnetic field in the radio frequency spectrum that is caused by another electronic device.

EPROM means erasable Programmable Read Only Memory—a non-volatile storage chip or device that may be filled with data and information, that, once written, is not modifiable, and that is retained even if there is no power applied to the system.

Exception report means a listing of occurrences, transactions or items that fall outside a predetermined range of acceptability.

Financial instrument means any tangible item of value tendered in game play, including, but not limited to bills, coins, vouchers, and coupons.

Financial instrument storage component (or Drop Box) means any component that stores financial instruments, such as a drop box, but typically used in connection with player interfaces.

FinCEN means Financial Crimes Enforcement Network, Department of the Treasury.

Fill means a transaction whereby a supply of cash, chips or coins is transferred from the cage to a table game, cashier station, bingo, pull tab, OTB, or keno department.

Fill Slip means a document evidencing a fill.

Game software means the operational program or programs that govern the play, display of results, and/or awarding of prizes or credits for games.

Gaming system means all components, whether or not technologic aids in electronic, computer, mechanical, or other technologic form, that function together to aid the play of Class II and Class III games, including accounting functions mandated by these regulations or part 547 of this chapter.

Gaming equipment means all electronic, electro-mechanical, mechanical, or other physical components utilized in the play of games.

Gaming promotion means any promotional activity or award that requires game play as a condition of eligibility.

Gaming means staking or risking something of value upon the outcome of a contest of chance or a future contingent event not under the person's control or influence, upon an agreement or understanding that the person or someone else will receive something of value in the event of a certain outcome.

Generally Accepted Accounting Principles (GAAP) means a widely accepted set of rules, conventions, standards, and procedures for reporting financial information, as established by the Financial Accounting Standards Board (FASB), including, but not limited to, the standards for casino accounting published by the American Institute of Certified Public Accountants (AICPA).

Generally Accepted Auditing Standards (GAAS) means a widely accepted set of standards that provide a measure of audit quality and the objectives to be achieved in an audit, as established by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA).

Governmental Accounting Standards Board (GASB) means generally accepted accounting principles used by state and local governments.

Gross Gaming Revenue means annual total amount of money wagered on Class II and Class III games and admission fees (including table or card fees), less any amounts paid out as prizes or paid for prizes awarded.

Hardware means gaming equipment.

Hold means the relationship of win to credit or ticket-in for EGM's and win to drop for table games.

Imprest Basis means a method of accounting for a cash or cash equivalent bank such that the expected value remains a constant, fixed, and known amount.

Independent means the separation of functions to ensure that the agent or process monitoring, reviewing, or authorizing the controlled activity, function, or transaction is separate from the agents or process performing the controlled activity, function, or transaction.

Inspector means an employee of the Tribal Gaming Agency duly appointed by the agency as an Inspector.

Internal Audit means individuals who are independent of gaming operations with respect to the departments subject to audit (auditors internal to the operation, officers of the TGRA, or outside CPA firm may perform this function). Internal auditor(s) report directly to the Tribe, TGRA, audit committee, or other entity designated by the Tribe.

Jackpot Payout means the portion or amount of a jackpot paid by EGM personnel.

Kiosk means a device capable of redeeming vouchers and/or wagering credits or initiating electronic transfers of money to or from a patron deposit account.

Main Card Room Bank means a fund of currency, coin, and chips used primarily for poker card game areas. Used to make even money transfers between various games as needed. May be used similarly in other areas of the gaming operation. May also be known as the Cage Poker Window.

Manual payout means any non-automated payout.

Master Game Program Number means the game program number listed on an EGM EPROM, or other equivalent game software media.

Master Game Report means a form used to record, by shift and day, each table game's winnings and losses. This form reflects the opening and closing table inventories, the fills and credits, and the drop and win. This form is also known as the "stiff sheet."

MICS means minimum internal control standards in this part.

Modification means a revision to any hardware or software used in a gaming system.

Network communication equipment means a device or collection of devices that controls data communication in a system including, but not limited to, cables, switches, hubs, routers, wireless access points, landline telephones and cellular telephones.

NIGC means the National Indian Gaming Commission, established by the Indian Gaming Regulatory Act, 25 U.S.C. 2701 et seq.

Non-cashable credit means credits given by an operator to a patron; placed on a Class II or Class III gaming system through a coupon, cashless transaction or other approved means; and capable of activating play but not being converted to cash.

Openers and Closers means the forms used by gaming operation supervisory personnel to document the inventory of chips and coins on a table at the beginning and ending of a shift and by Accounting to calculate the Table Games win/loss. Also known as a table inventory form/slip.

Patron means a person who is a customer or guest of the gaming operation and may interact with a game. Also may be referred to as a "player."

Par Percentage means the percentage of each dollar wagered that the house wins (i.e., gaming operation advantage).

Par Sheet means a manufacturer's specification sheet for an electronic lottery game that provides game payouts by type, count, and percentage.

Payout means a transaction associated with a winning event.

PIN means the personal identification number used to access a player's account.

Pit Supervisor means the employee who supervised all games in a pit.

Player Account Server means a system used by a gaming operation to monitor EGM activity on an online basis.

Player interface means any component(s) of a gaming system, including an electronic or technologic aid (not limited to terminals, player stations, handhelds, fixed units, etc.), that directly enables player interaction in a Class II or Class III game.

Player Supported Jackpot (PSJ) means a separate contest of chance directly related to the play or outcome of an authorized Table Game, Tribal Lottery System, or Electronic Bingo game. In PSJs, operations: (a) Collect funds from the players' wagers (the pot) for a separate prize; and (b) Act only as the custodian of the PSJ funds, including any interest earned on this money; and (c) Maintain no legal right to the funds, except for administrative fees; and (d) Must strictly account for all funds.

Player Tracking System means a system used in gaming departments to record the gaming activity of individual patrons.

Primary and Secondary Jackpots means promotional pools offered at certain card games that can be won in addition to the primary pot.

Prize payout means payment to a player associated with a winning or qualifying event.

Progressive prize means a prize that increases by a selectable or predefined amount based on play of a game.

Progressive Electronic Gaming Machine means an EGM, with a payoff indicator, in which the payoff increases as it is played (i.e., deferred payout). The payoff amount is accumulated, displayed, and remains until a player attains the pre-determined event that results in the progressive amount being paid.

Progressive Jackpots means deferred payout from a progressive EGM or table game.

Progressive Table game means table games that offer progressive jackpots.

Promotional Payouts generally means personal property or awards given to players by the gaming operation as an inducement to play. Promotions vary but a promotion example might be a program developed where a player receives a form of personal property based on the number of games or sessions played.

Promotional Progressive Pots/Pools means funds contributed to a game by and for the benefit of players that are distributed to players based on a predetermined event.

Proposition Player means a person paid a fixed sum by the gaming operation for the specific purpose of playing in a card game. A proposition player makes wages with her/his own funds, retains her/his winnings, and absorbs her/his losses.

Rake means a commission charged by the house for maintaining or dealing a game such as poker.

Rake Circle means the area of a table where the rake is placed.

Random number generator (RNG) means a software module, hardware component or combination of these designed to produce outputs that are effectively random.

Reflexive software means any software that has the ability to manipulate and/or replace a randomly generated outcome for the purpose of changing the results of a game.

Removable/rewritable storage media means program or data storage components that can be removed from gaming equipment and be written to, or rewritten by, the gaming equipment or by other equipment designed for that purpose.

Request for Fill means a form that is used to request the transfer of chips and/or coin from the cage to a table. The request precedes the actual transfer transaction that is documented on a fill slip.

Request for Credit means a form that is used to request the transfer of chips from a table to the cage.

The order precedes the actual transfer transaction that is documented on a credit slip.

Runner means a gaming employee who transports chips/cash between a gaming table and a cashier.

Server means a computer that controls one or more applications or environments within a gaming system.

Seed Money means a beginning jackpot amount (also known as a base amount) added to a progressive meter which the operation funds, but maybe recovered by the operation through player funds once per seed amount the operation contributes.

Shift means a time period, unless otherwise approved by the Tribal Gaming Agency, not to exceed 24 hours.

Shill Funds means financing provided by the gaming operation to a proposition player.

Signature (as required upon any record or document) means the legible recording in script of not less than a person's first initial, last name, and certificate or permit number.

Soft Count means the count of the contents in a drop box or currency acceptor.

Sufficient clarity means the capacity of a surveillance system to record images at a minimum of 20 frames per second or equivalent recording speed and at a resolution sufficient to clearly identify the intended activity, person, object, or location.

Surveillance operation room(s) means the secured area(s) where surveillance takes place and/or where active surveillance equipment is located.

Surveillance system means a system of video cameras, monitors, recorders, video printers, switches, selectors, and other equipment used for surveillance.

SICS (System of Internal Control Standards) means an overall operational framework for a gaming operation that incorporates principles of independence and segregation of function, and is comprised of written policies, procedures, and standard practices based on overarching regulatory standards specifically designed to create a system of checks and balances to safeguard the integrity of a gaming operation and protect its assets from unauthorized access, misappropriation, forgery, theft, or fraud.

Table Games means games that are banked by the house or a pool whereby the house or the pool pays all winning bets and collects from all losing bets.

Table Inventory means total coins and chips at a Table.

Table Inventory Form means the document where chips and funds held at a table are recorded when table inventory is taken. Also known as a table inventory slip and openers and closers.

Test/diagnostics mode means a mode on a component that allows various tests to be performed on the gaming system hardware and software.

Testing lab means an organization recognized by a TGA pursuant to § 547.5(f) and the Tribal-State Compact.

TGA means the Tribal Gaming Agency, which is the entity authorized by tribal law to regulate gaming conducted pursuant to the Indian Gaming Regulatory Act.

TGO means the Tribal Gaming Operations (operation or gaming operation) refers to the Ilani Casino.

Theoretical Hold means the intended hold percentage or win as computed and referenced to its payout schedule or par sheet.

Theoretical Hold Worksheet means a worksheet provided by the manufacturer that indicates the theoretical percentages that the gaming device should hold based on exhaustive play.

Tier A means gaming operations with annual gross gaming revenues of more than $3 million but not more than $8 million.

Tier B means gaming operations with annual gross gaming revenues of more than $8 million but not more than $15 million.

Tier C means gaming operations with annual gross gaming revenues of more than $15 million.

TICS means the Tribal Internal Control Standards established by the TGA that are at least as stringent as the standards set forth in the Tribal State Compact and 25 CFR Part 542 and 543.

Tribal-State Compact means an agreement between a tribe and a state to govern the conduct of Class III gaming

Vault means a secure area where cash and cash equivalents are stored.

Voucher means a financial instrument of fixed wagering value, usually paper, that can be used only to acquire an equivalent value of cashable credits or cash through interaction with a voucher system.

Voucher system means a system that securely maintains records of vouchers and coupons; validates payment of vouchers; records successful or failed payments of vouchers and coupons; and controls the purging of expired vouchers and coupons.

Wide Area Progressive Electronic Gaming Machine means a Class II progressive EGM that makes deferred payouts where individual machines are linked to machines in other operations and all the machines affect the progressive amount. As money is inserted into a single machine, the progressive meter on all of the linked machines increases.

Win means the net win resulting from all gaming activities. Net win results from the total amount of gaming income (gross gaming revenue) after prizes or winnings have been paid out; i.e., the difference between the total amount wagered or played and the amounts repaid to the winners.

WSGC means the Washington State Gambling Commission

## 3.1. System of Internal Control Standards (SICS) MICS 542.3(d)

A. The Tribal Gaming Operations (TGO) must develop and implement a System of Internal Control Standards (SICS) that, at a minimum, complies with the TICS.

B. Initially and upon each subsequent update of the SICS, TGO shall submit the SICS document to the Tribal Gaming Agency for review, discussion, and approval.

C. All changes necessary to ensure compliance with the TICS must be promulgated and implemented no later than 30 days after final approval by TGA.

## 3.2. Alternate Minimum Standards MICS 542.18

A. The gaming operation may request an alternate standard from those set forth in the TICS if the gaming operation:

1. Determines that it is unable to comply substantially with a standard in the TICS; and
2. Develops an alternate standard that will achieve at least the same level of control for the standard that it seeks to replace.

B. For each standard for which the gaming operation seeks an alternate, the gaming operation shall submit to TGA a detailed report which shall include the following information:

1. An explanation of why the gaming operation is unable to comply substantially with the standard;
2. A description of the proposed alternate standards; and
3. An explanation of how the proposed alternate standard achieves at least the same level of control as the standard it is to replace.

C. TGA may test the adequacy of the alternate standards.

D. TGA may approve an alternate standard from those required if it has determined that the alternate standard will achieve a level of security and integrity sufficient to accomplish the purpose of the standard it is to replace. A gaming operation may implement an alternate standard upon approval by TGA.

E. For each applicable enumerated standard for which TGA approves an alternate standard, it must submit to the Chair of NIGC within 30 days a detailed report and to the WSGC, which must include the following:

1. An explanation of how the alternate standard achieves a level of security and integrity sufficient to accomplish the purpose of the standard it is to replace; and

2. The alternate standard as approved and the record on which it is based.

F. Chair of NIGC review

Under IGRA there are circumstances in which the NIGC Chair may be required to approve certain CTGC or ilani regulations, these may include: the process to license key employees and facility licenses as defined under IGRA and NIGC; Tribal Gaming Ordinances; Management contracts; Net Gaming Revenues; Environmental, Public Health and Safety.

1. The Chair may approve or object to an alternate standard approved by TGA.
2. If the Chair approves the alternate standard, the TGO may continue to use it as authorized by the TGA.
3. If the Chair objects, the TGO may no longer use the alternate standard and must follow the relevant internal controls set forth in the TICS.
4. Any objection by the Chair must be in writing and provide reasons that the alternate standard, as approved by the TGA, does not provide a level of security or integrity sufficient to accomplish the purpose of the standard it is to replace.
5. If the Chair fails to approve or object in writing within 60 days after the date of receipt of a complete submission, the alternate standard is considered approved by the Chair. The Chair may, upon notification to the TGA, extend this deadline an additional 60 days.

G. WSGC review

1. TGA shall notify the WSGC of any intent to revise Class III standards or of any other regulations issued thereafter and shall request the concurrence of the WSGC for such revisions. WSGC and TGA shall agree upon the alternative standards according to the provisions of the TSC Section IX.A(3)

## 3.3. Variances

A. Where referenced throughout the TICS, TGO must set a reasonable threshold, approved by TGA, for when a variance must be reviewed to determine the cause, and the results of the review must be documented and maintained.

B. If TGA determines there is a pattern or excessive number of variances which do not meet the established threshold, TGA may request, and the TGO must comply, with an adjusted threshold.

## 3.4. Certified Public Accountant (CPA) MICS 543.23

A. The Certified Public Accountant (CPA) shall perform an independent assessment to verify whether the TGO's SICS is in substantial compliance with the TICS by comparing the documents.

B. The CPA shall also perform an independent assessment to verify whether the TGO has implemented and is in substantial compliance with its SICS. These procedures may be performed in conjunction with the annual audit.

C. The CPA shall prepare a report of the material weakness in accounting and system of internal controls for the Tribe and management.

D. Tribal Gaming Operation shall submit two copies of the CPA's agreed-upon procedures report of TGO's compliance to NIGC within 120 days of TGO's fiscal year end in conjunction with the submission of the annual financial audit report.

E. If the CPA determines that the internal audit procedures performed during the fiscal year have been properly completed, the CPA may rely on the work of the internal audit for the completion of the MICS checklists as they relate to the standards in A and B above with agreement of the Tribal Gaming Agency.

## 3.5. Records, Documents and Retention

A. The TGO shall keep permanent books of account or records, including inventory records of gaming supplies, sufficient to establish the amount of gross and net revenue, deductions and expenses, receipts and disbursements, and other information required in any financial statement, report, and/or other accounting records prepared pursuant to these standards. **TSC App.A:4(1); App. A:4(4)**

B. These books or records shall be kept at all times and made readily available upon request for inspection by the authorized representatives of TGA.

C. Except as otherwise specified in these standards, all required records, reports, and documents shall be retained for a period of at least five (5) years in a manner that assures reasonable accessibility. MICS 542.19(k)

D. Access logs and authorization lists shall be retained for a period of at least two (2) years in a manner that assures reasonable accessibility. **TSC App.A:4(5)**

## 3.6. Established Procedures

A. TGO shall submit initially, and upon each subsequent update, for review, discussion, and approval, all procedures established pursuant to the standards of the TICS.

B. Any requirement for the establishment of procedures pursuant to the standards of TICS must be submitted to TGA no later than 30-days following the effective date or thereafter within 20-days of TGA request. Effective dates for updates

shall be upon approval of TGA unless otherwise specified by TGA.

## 3.7. Computer Applications

A. For any computer applications utilized, alternate documentation and/or procedures that provide at least the level of control established by the standards of this part, as approved in writing by TGA will be acceptable. MICS 542.12(a); 542.13(b); 542.14(a); 542.41(a)

B. For Class III gaming, in addition to TGA's approval, for any computer application utilized, alternate documentation and/or procedures that provide at least the level of control established by the Tribal-State Compact need concurrence with the WSGC. **TSC App. A :17(9)**

# Chapter 4 Bingo Minimum Internal Control Standards

## 4.1. Supervision

A. Supervision must be provided as required for bingo operations by an agent(s) with authority greater than those being supervised. **(MICS 543.8(a))**

B. Key management personnel shall be on the premises at which the bingo game is licensed for operation, during all hours of its operation. Such personnel shall be of a position of shift-manager or higher and hold a current and valid license from the TGA. Such hours of operation shall include at a minimum any time during which the premises are open to the public for entrance and occupation.

## 4.2. Bingo Card Sales MICS 543.8(c)(4)(i-v)

A. In order to adequately record, track and reconcile sales of bingo cards, the following information must be documented from the server (this is not required if the system does not track the information, but system limitation(s) must be noted):

1. Date;
2. Time;
3. Number of bingo cards sold;
4. Dollar amount of bingo card sales; and
5. Amount in, amount out and other associated meter information.

## 4.3. Draw MICS 543.8(d)(2-4)(i-ii)

A. Where the selection is made through an electronic aid, certification in accordance with 25 CFR 547.14 is acceptable for verifying the randomness of the draw and satisfies the requirements of paragraph (d)(1) of this section.

B. Controls must be established and procedures implemented to provide a method of recall of the draw, which includes the order and identity of the objects drawn, for dispute resolution purposes.

C. Verification and display of draw. Controls must be established and procedures implemented to ensure that:

1. The identity of each object drawn is accurately recorded and transmitted to the participants. The procedures must identify the method used to ensure the identity of each object drawn.
2. For all games offering a prize payout of $1,200 or more, as the objects are drawn, the identity of the objects are immediately recorded and maintained for a minimum of 24 hours.

## 4.4. Prize Payout

A. Controls must be established and procedures implemented for cash or cash equivalents that address the following: **(MICS 543.8(e)(1))**

1. Identification of the agent authorized (by position) to make a payout;
2. Predetermined payout authorization levels (by position); and
3. Documentation procedures ensuring separate control of the cash accountability functions.

B. Verification of validity. **(MICS 543.8(e)(2))**

1. Controls must be established and procedures implemented to verify that the following is valid for the game in play prior to payment of a winning prize:
   a) Winning card(s);
   b) Objects drawn; and
   c) The previously designated arrangement of numbers or designations on such cards.
2. At least two agents must verify that the card, objects drawn, and previously designated arrangement were valid for the game in play.
3. Where an automated verification method is available, verification by such method is acceptable.

C. Validation. **(MICS 543.8(e)(3))**

1. For manual payouts, at least two agents must determine the validity of the claim prior to the payment of a prize. The system may serve as one of the validators.
2. For automated payouts, the system may serve as the sole validator of the claim.

D. Verification. **(MICS 543.8(e)(4))**

1. For manual payouts, at least two agents must verify that the winning pattern has been achieved on the winning card prior to the payment of a prize. The system may serve as one of the verifiers.
2. For automated payouts, the system may serve as the sole verifier that the pattern has been achieved on the winning card.

E. Authorization and signatures. **(MICS 543.8(e)(5))**

1. At least two agents must authorize, sign, and witness all manual prize payouts above $1,200, or a lower threshold as authorized by management and approved by the TGA.
2. Manual prize payouts above the following threshold (or a lower threshold, as authorized by management and approved by TGA) must

require one of the two signatures and verifications to be a supervisory or management employee independent of the operation of Class II Gaming System bingo:

a) $5,000 for a Tier A facility;

b) $10,000 at a Tier B facility;

c) $20,000 for a Tier C facility; or

d) $50,000 for a Tier C facility with over $100,000,000 in gross gaming revenues

3. The predetermined thresholds, whether set at the TICS level or lower, must be authorized by management, approved by TGA, documented, and maintained.

4. A Class II gaming system may substitute for one authorization/signature verifying, validating or authorizing a winning card, but may not substitute for a supervisory or management authorization/signature.

F. Payout records, including manual payout records, must include the following information: **(MICS 543.8(e)(6))**

1. Date and time;

2. Amount of the payout (alpha & numeric for player interface payouts); and

3. Bingo card identifier or player interface identifier.

4. Manual payout records must also include the following:

a) Game name or number;

b) Description of pattern covered, such as cover-all or four corners;

c) Signature of all, but not less than two, agents involved in the transaction;

d) For override transactions, verification by a supervisory or management agent independent of the transaction; and

e) Any other information necessary to substantiate the payout.

## 4.5. Cash and Cash Equivalent Controls MICS 543.8(f)

A. Cash or cash equivalents exchanged between two persons must be counted independently by at least two agents and reconciled to the recorded amounts at the end of each shift or session. Unexplained variances must be documented and maintained. Unverified transfers of cash or cash equivalents are prohibited.

B. Procedures must be implemented to control cash or cash equivalents based on the amount of the transaction. These procedures must include documentation by shift, session, or other relevant time period of the following:

1. Inventory, including any increases or decreases;

2. Transfers;
3. Exchanges, including acknowledging signatures or initials; and
4. Resulting variances.

C. Any change to control of accountability, exchange, or transfer requires that the cash or cash equivalents be counted and recorded independently by at least two agents and reconciled to the recorded amount.

## 4.6. Technologic Aids to the Play of Bingo MICS 543.8(g)

A. Controls must be established, and procedures implemented to safeguard the integrity of technologic aids to the play of bingo during installations, operations, modifications, removal and retirements. Such procedures must include the following:

1. Shipping and receiving

a) A communication procedure must be established between the supplier, the gaming operation, and TGA to properly control the shipping and receiving of all software and hardware components. Such procedures must include:

(1) Notification of pending shipments must be provided to TGA by the gaming operation;
(2) Certification in accordance with 25 CFR part 547;
(3) Notification from the supplier to TGA, or the gaming operation as approved by TGA, of the shipping date and expected date of delivery. The shipping notification must include:

(i) Name and address of the supplier;
(ii) Description of shipment;
(iii) For player interfaces: a serial number;
(iv) For software: software version and description of software;
(v) Method of shipment; and
(vi) Expected date of delivery.

b) Procedures must be implemented for the exchange of the gaming system components for maintenance and replacement.

c) Gaming system components must be shipped in a secure manner to deter unauthorized access.

d) TGA, or its designee, must receive all the gaming system components and game play software packages, and verify the contents against the shipping notification.

2. Access credential control methods.

a) Controls must be established to restrict access to the gaming system components.

3. Recordkeeping and audit processes.

   a) The gaming operation must maintain the following records, as applicable, related to installed game servers and player interfaces:

      (1) Date placed into service;
      (2) Date made available for play;
      (3) Supplier;
      (4) Software version;
      (5) Serial number;
      (6) Game title;
      (7) Asset and/or location number;
      (8) Seal number; and
      (9) Initial meter reading.

   b) Procedures must be implemented for auditing such records in accordance with §543.23, Audit and Accounting.

4. System software signature verification.

   a) Procedures must be implemented for system software verifications. These procedures must include comparing signatures generated by the verification programs required by 25 CFR 547.8, to the signatures provided in the independent test laboratory letter for that software version.

   b) An agent independent of operation must perform system software signature verification(s) to verify that only approved software is installed.

   c) Procedures must be implemented for investigating and resolving any software verification variances.

   d) Internal audits must be conducted. Such audits must be documented.

5. Installation testing.

   a) Testing must be completed during the installation process to verify that the player interface has been properly installed. This must include testing of the following, as applicable:

      (1) Communication with the gaming system;
      (2) Communication with the accounting system;
      (3) Communication with the player tracking system;
      (4) Currency and vouchers to bill acceptor;
      (5) Voucher printing;
      (6) Meter incrimination;
      (7) Pay table, for verification;
      (8) Player interface denomination, for verification;
      (9) All buttons, to ensure that all are operational and programmed

appropriately;

(10) System components, to ensure that they are safely installed at location; and

(11) Locks, to ensure that they are secure and functioning.

6. Display of rules and necessary disclaimers.

   a) The operation must ensure that all game rules and disclaimers are displayed at all times or made readily available to the player upon request,

   b) TGA must verify that all game rules and disclaimers are displayed at all times or made readily available to the player upon request, as required by 25 CFR part 547

7. TGA approval of all technologic aids before they are offered for play.

8. All Class II gaming equipment must comply with 25 CFR part 547, Minimum Technical Standards for Gaming Equipment Used with the Play of Class II Games; and

9. Dispute resolution.

## 4.7. Operations MICS 543.8(h)

A. Malfunctions - Procedures must be implemented to investigate, document and resolve malfunctions. Such procedures must address the following:

1. Determination of the event causing the malfunction;

2. Review of relevant records, game recall, reports, logs, surveillance records;

3. Repair or replacement of the gaming component;

4. Verification of the integrity of the gaming component before restoring it to operation.

B. Removal, retirement and/or destruction. Procedures must be implemented to retire or remove any or all associated components of a gaming system from operation. Procedures must include the following:

1. For player interfaces and components that accept cash or cash equivalents:

   a) Coordinate with the drop team to perform a final drop;

   b) Collect final accounting information such as meter readings, drop and payouts;

   c) Remove and/or secure any or all associated equipment such as locks, card reader, or ticket printer from the retired or removed component; and

   d) Document removal, retirement, and/or destruction.

2. For removal of software components:

a) Purge and/or return the software to the license holder; and

b) Document the removal.

3. For other related equipment such as blowers, cards, interface cards:

a) Remove and/or secure equipment; and

b) Document the removal or securing of equipment.

4. For all components:

a) Verify that unique identifiers, and descriptions of removed/retired components are recorded as part of the retirement documentation; and

b) Coordinate with the accounting department to properly retire the component in the system records.

5. Where TGA authorizes destruction of any gaming system components, procedures must be developed to destroy such components. Such procedures must include the following:

a) Methods of destruction;

b) Witness or surveillance of destruction;

c) Documentation of all components destroyed; and

d) Signatures of agent(s) destroying components attesting to destruction

## 4.8. Vouchers MICS 543.8(i)

A. Controls must be established and procedures implement to:

1. Verify the authenticity of each voucher redeemed.

2. If the voucher is valid, verify that the patron is paid the appropriate amount.

3. Document the payment of a claim on a voucher that is not physically available or a voucher that cannot be validated such as a mutilated, expired, lost, or stolen voucher.

4. Retain payment documentation for reconciliation purposes.

5. For manual payment of a voucher of $500 or more, require a supervisory employee to verify the validity of the voucher prior to payment.

B. Vouchers paid during a period while the voucher system is temporarily out of operation must be marked “paid” by the cashier.

C. Vouchers redeemed while the voucher system was temporarily out of operation must be validated as expeditiously as possible upon restored operation of the voucher system.

D. Paid vouchers must be maintained in the cashier's accountability for reconciliation purposes.

E. Unredeemed vouchers can only be voided in the voucher system by supervisory employees. The accounting department will maintain the voided voucher, if available.

## 4.9. Variance MICS 543.8(l)

A. The operation must establish, as approved by TGA, the threshold level of at least +/- 3%, at which a variance, including deviations from the mathematical expectations required in this section, will be reviewed to determine the cause. Any such review must be documented.

1. Fairness. No gaming system may cheat or mislead users. All prizes advertised must be available to win during the game. A test laboratory must calculate and/or verify the mathematical expectations of game play, where applicable, in accordance with the manufacturer stated submission. The results must be included in the test laboratory's report to TGA.

# Chapter 5 CARD GAMES

## 5.1. Supervision

A. Supervision must be provided as required during the card room operations by an agent(s) with authoritygreater than those being supervised.

1. A supervisor may function as a dealer without any other supervision if disputes are resolved, and exchanges and transfers are authorized by other supervisory agents.
2. A dealer may function as a supervisor if not dealing the game.

## 5.2. Exchanges or Transfers

A. Exchanges between table banks and the main card room bank (or cage, if a main card room bank is not used) must be authorized by a supervisor. All exchanges must be evidenced by the use of a lammer unless the exchange of chips, tokens, and/or cash takes place at the table. If table banks are maintained at an imprest level and runners are used for the exchanges at the table, no supervisory authorization is required.

B. Exchanges from the main card room bank (or cage, if a main card room bank is not used) to the table banks must be verified by the card room dealer and the runner.

C. Transfers between the main card room bank and the cage must be properly authorized and documented. Documentation must be retained for at least 24 hours.

## 5.3. Playing Cards

A. New and used playing cards must be maintained in a secure location, with appropriate surveillance coverage, and accessible only to authorized agents.

B. Used playing cards that are not to be re-used must be properly cancelled and removed from service to prevent re-use. The removal and cancellation procedure requires TGA review and approval.

C. Playing cards associated with an investigation must be retained intact and outside of the established removal and cancellation procedure.

## 5.4. Shill Funds

A. Issuance of shill funds must be recorded and have the written approval of the supervisor.

B. Returned shill funds must be recorded and verified by a supervisor.

C. The replenishment of shill funds must be documented.

## 5.5. Reconciliation of Card Room Bank

A. Two agents—one of whom must be a supervisory agent—must independently count the table inventory at the opening and closing of the table and record the following information:

1. Date;
2. Shift;
3. Table number;
4. Amount by denomination;
5. Amount in total; and
6. Signatures of both agents.

## 5.6. Posted Rules

A. The rules must be displayed or available for patron review at the gaming operation, including rules governing contests, prize payouts, fees, the rake collected, and the placing of antes.

1. Prohibitions on side betting between and against player and against the house.

## 5.7. Promotional Progressive Pots and Pools

A. All funds contributed by players into the pools must be returned when won in accordance with posted rules, and no commission or administrative fee may be withheld.

1. The payout may be in the form of personal property, such as a car.
2. A combination of a promotion and progressive pool may be offered.

B. The conditions for participating in current card game promotional progressive pots and/or pools must be prominently displayed or available for patron review at the gaming operation.

C. Individual payouts for card game promotional progressive pots and/or pools that are $600 or more must be documented at the time of the payout to include the following:

1. Patron's name;
2. Date of payout;
3. Dollar amount of payout and/or nature and dollar value of any non-cash payout;
4. The signature of the agent completing the transaction attesting to the disbursement of the payout; and

5. Name of contest/tournament.

D. If the cash (or cash equivalent) payout for the card game promotional progressive pot and/or pool is less than $600, documentation must be created to support accountability of the bank from which the payout was made.

E. Rules governing current promotional pools must be conspicuously posted in the card room and/or available in writing for patron review. The rules must designate:

1. The amount of funds to be contributed from each pot;
2. What type of hand it takes to win the pool;
3. How the promotional funds will be paid out;
4. How/when the contributed funds are added to the pools; and
5. Amount/percentage of funds allocated to primary and secondary pools, if applicable.

F. Promotional pool contributions must not be placed in or near the rake circle, in the drop box, or commingled with gaming revenue from card games or any other gambling game.

G. The amount of the pools must be conspicuously displayed in the card room.

H. At least once each day that the game is offered, the posted pool amount must be updated to reflect the current pool amount.

I. At least once each day that the game is offered, agents independent of the card room must reconcile the increases to the posted pool amount to the cash previously counted or received by the cage.

J. All decreases to the pool must be properly documented, including a reason for the decrease.

K. Promotional funds removed from the card game must be placed in a locked container.

1. Agents authorized to transport the locked container are precluded from having access to the contents keys.
2. The contents key must be maintained by a department independent of the card room.
3. At least once a day, the locked container must be removed by two agents, one of whom is independent of the card games department, and transported directly to the cage or other secure room to be counted, recorded, and verified, prior to accepting the funds into cage accountability.

## 5.8. Accepting Cash at Gaming Stations

A. The cash shall be spread on the top of the gaming station by the dealer or croupier, accepting it in full view of the patron who presented it and the supervisor specifically assigned to such gaming station.

B. The amount of cash shall be announced by the dealer or croupier accepting it in a tone of voice calculated to be heard by the patron who presented the cash and the supervisor specifically assigned to such gaming station. All cash changes of $100 or over shall be verified by the supervisor.

C. Immediately after an equivalent amount of gaming chips has been given to the patron, the cash shall be taken from the top of the gaming station and placed by the dealer or croupier into the drop box attached to the gaming station.

## 5.9. Acceptance of Gratuities from Patrons

A. No tribal gaming operation employee directly concerned with management, accounting, security and surveillance shall solicit or accept any tip or gratuity from any player or patron.

B. The tribal gaming operation shall establish a procedure for accounting for all tips received by other gaming employees.

C. Upon receipts from a patron of a tip, a dealer assigned to a gaming station shall tap the table or wheel and extend his or her arm to show the supervisor that he has received a tip and immediately deposit such tip in the tip box. Tips received shall be retained by employees or pooled among employees in such a manner as determined by the TGO.

# Chapter 6 GAMING PROMOTIONS & PLAYER TRACKING

## 6.1. Supervision MICS 543.12(a)

A. Supervision must be provided as required for gaming promotions and player tracking by an agent(s) with authority greater than those being supervised.

## 6.2. Gaming promotions 543.12(b)

A. The rules of the gaming promotion must be displayed or made readily available to patron upon request. Gaming promotions rules require TGA approval and must include the following:

1. The rules of play;
2. The nature and value of the associated prize(s) or cash award(s);
3. Any restrictions or limitations on participant eligibility;
4. The date(s), time(s), and location(s) for the associated promotional activity or activities;
5. Any other restrictions or limitations, including any related to the claim of prizes or cash awards;
6. The announcement date(s), time(s), and location(s) for the winning entry or entries; and
7. Rules governing promotions offered across multiple gaming operations, third party sponsored promotions, and joint promotions involving third parties.

## 6.3. Player Tracking Systems and Gaming Promotions 543.12(c)

A. Changes to the player tracking systems, promotion and external bonusing system parameters, which control features such as the awarding of bonuses, the issuance of cashable credits, non-cashable credits for gaming, coupons and vouchers, must be performed under the authority of supervisory agents, independent of the department initiating the change. Alternatively, the changes may be performed by supervisory agents of the department initiating the change with notification of TGA, if sufficient documentation is generated and the propriety of the changes are verified by supervisory agents independent of the department initiating the change.

B. All other changes to the player tracking system must be appropriately documented.

## 6.4. Player Tracking System Controls MICS 543.12(c)(2)

A. The player tracking system shall be secured so as to prevent unauthorized access (e.g., changing passwords at least quarterly and physical access to computer hardware, etc.).

B. The addition of points to members' accounts other than through actual gaming play shall be sufficiently documented (including substantiation of reasons for increases). Each request shall be in writing by the department determining an adjustment is necessary. The written request shall be forwarded to a designated person or group within accounting, as designated by the operation, who will review and (if appropriate) authorize the adjustment. Authorized point adjustments shall then be forwarded to Marketing or Player Services staff as designated by the operation. This employee may not have the ability to either create player's club accounts or issue momentum cards.

C. Employees who redeem points for members shall not have access to lost cards.

# Chapter 7 TABLE GAMES

## 7.1. Supervision

A. Pit supervisory personnel (with authority equal to or greater than those being supervised) shall provide supervision of all table games.

## 7.2. Table Inventory Requirements and Procedures TSC App. A:16(1-4)

A. Station inventory slips shall be a pre-numbered, three-part form, “Opener,” “Closer,” and triplicate, which are maintained and controlled by security. The Gaming Facility supervisor shall record the following:

1. The date and identification of the shift ended;
2. The game and station number;
3. The value of each denomination of gaming chips and coins, and total.
4. Signatures shall be of either the Dealer and the Gaming Facility supervisor assigned to the incoming and outgoing shifts or the Gaming Facility supervisor assigned to the gaming station at the time of a Drop Box shift change and another table games employee.

B. Each station inventory and the Opener shall be stored while not in use in a separate locked, clear container which shall be clearly marked on the outside with the game and the gaming station number to which it corresponds. The information on the Opener shall be visible from the outside of the container. All containers shall be stored either in the cashier's cage or secured to the gaming station while not in use.

C. The keys to the locked containers containing the station inventories shall be maintained and controlled by the Gaming Facility department in a secure place and will not be accessible to any cashier's cage or security personnel.

D. Gaming chips or coins cannot be added to or removed from station inventory during the gaming day except:

1. In exchange for cash;
2. In payment of winning wagers and collection of losing wagers made at such gaming station;
3. In exchange for gaming chips received from a patron having an equal aggregate face value; and
4. In conformity with the fill and credit procedures described in these standards.

## 7.3. Procedures for Opening Stations for Gaming TSC App. A:16(5)

A. Gaming stations will be opened for gaming activity as follows:

1. The inventory container shall be unlocked in the presence of the Gaming

Facility supervisor.

2. A Dealer shall count the contents of the container in the presence of the Gaming Facility supervisor and shall verify the count to the Opener removed from the container.
3. The Dealer and the Gaming Facility supervisor will sign the Opener.
4. Any discrepancy between the table inventory and the Opener shall be immediately reported to at least the Gaming Facility shift manager, the security department, and the Tribal Gaming Agency Inspector. A Notification of Error (NOE) or security report shall be completed in conformity with agreed upon internal controls. In the event a security report is written; a copy must be forwarded to accounting for reconciliation purposes.
5. After the count of the contents of the container and the signing of the Opener, it shall be immediately deposited in the Drop Box attached to the gaming station by the Dealer.

## 7.4. Procedures for Closing Gaming Stations TSC App. A:16(6-7)

A. When gaming activity at a gaming station is concluded, the gaming chips and coins shall be counted by the Dealer assigned to the gaming station and observed by a table games supervisor.

B. The gaming chips and coins counted shall be recorded on a station inventory slip by the table games supervisor

C. The Dealer and the table games supervisor, who observed the Dealer count, will sign the station inventory slip.

D. Upon meeting the signature requirements, the Closer shall be deposited in a Drop Box attached to the gaming station immediately prior to the closing of the station.

E. The triplicate copy of the station inventory slip shall be forwarded to the cashier's cage by a Security Department Member.

F. The Opener and the gaming chips remaining at the station shall be stored as outlined in 7.2B.

## 7.5. Fill and Credit General Standards MICS 542.12(c)(1-4)

A. Fill slips and credit slips shall be in at least triplicate form, in a continuous numerical series, and pre-numbered and concurrently numbered in a form utilizing the alphabet and only in one series at a time. The alphabet need not be used if the numerical series is not repeated during the business year.

B. Unissued and issued fill/credit slips shall be safeguarded and adequate

procedures shall be employed in the distribution, use, and control of unissued and issued fill/credit slips. Personnel from the cashier or pit departments shall have no access to the secured copies of the fill/credit slips.

C. When a fill/credit slip is voided, the cashier shall clearly mark "void" across the face of the original and first copy. The cashier and one other person independent of the transactions shall sign both the original and first copy, and shall submit them to the accounting department for retention and accountability.

D. Fill transactions shall be authorized by pit supervisory personnel before the issuance of fill slips and transfer of chips, tokens, or cash equivalents. The fill request shall be communicated to the cage where the fill slip is prepared.

E. Table credit transactions shall be authorized by a pit supervisor before the issuance of credit slips and transfer of chips, tokens, or other cash equivalent. The credit request shall be communicated to the cage where the credit slip is prepared. MICS 542.12(c)(12)

## 7.6. Fill Slip Standards

A. When table fills are transacted, a two-part request for fill shall be prepared by the pit supervisor for transferring chips, or monetary equivalents from the cage to the pit. TSC App. A:17(1)(a) and (c); MICS 542.12(c)(4)

B. The duplicate of the fill request form shall be retained in the pit to check the fill slip for proper entries and to document the total amount of chips and monetary equivalents to be added to the table inventory. TSC App.A:17(1)(c)(vi)

C. The original of the fill request shall be communicated to the cage where the fill slip is prepared. MICS 542.12(c)(4)

D. At least three parts of each fill slip shall be utilized as follows: MICS 542.12(c)(5)

1. Two parts shall be transported to the pit with the fill and, after the appropriate signatures are obtained, one part shall be deposited in the table drop box with the fill request duplicate;
2. One part shall be retained in the cage for reconciliation of cashier bank once signed by all participants and returned to the Cage by security; and
3. One part shall be retained intact by the locked machine in a continuous unbroken form. PROVIDED, for an automated system, the restricted copy may be retained within the automated system.

E. The part of the fill slip that is placed in the drop box shall be of a different color for fills than for credits, unless the type of transaction is clearly distinguishable in another manner (the checking of a box on the form shall not be a clearly distinguishable indicator). MICS 542.12(c)(6)

F. The game, table number, shift, and amount of fill by denomination and in total shall be noted on all copies of the fill slip. The correct date and time shall be indicated on at least two copies. 542.12(c)(7)

G. All fills shall be carried from the cashier's cage by a Security Department member. 542.12(c)(8)

H. The fill slip shall be signed by at least the following individuals (as an indication that each has counted the amount of the fill and the amount agrees with the fill slip): MICS 542.12(c)(9)

1. Cashier who prepared the fill slip and issued the chips, tokens, or monetary equivalent;
2. Security Department member who carried the chips, tokens, or monetary equivalents from the cage to the pit;
3. Dealer who received the chips, tokens, or monetary equivalents at the gaming table; and
4. Gaming Facility supervisor who supervised the fill transaction.

I. Fills shall be either broken down or verified by the dealer in public view before the dealer places the fill in the table tray. MICS 542.12(c)(10)

J. All fill slips requesting chips or money shall be prepared at the time a fill is made.

K. A copy of the fill slip shall then be deposited with the fill request duplicate into the drop box on the table by the dealer, where it shall appear in the count room with the cash receipts for the shift. MICS 542.12(c)(12); TSC App. A:17(6)(c)

## 7.7. Credit Slip Standards

A. When table credits are transacted, a two-part request for credit shall be prepared by the pit supervisor for transferring chips, tokens, or monetary equivalents from the pit to the cashier area or other secure area of accountability. TSC App. A:17(1)(a) and (c); MICS 542.12(c)(12)

B. The duplicate copy of a request for credit shall be retained in the pit to check the credit slip for proper entries and to document the total amount of chips, tokens, and monetary equivalents removed from the table. TSC App. A:17(1)(c)(vi)

C. The original of the credit request shall be communicated to the cage where the credit slip is prepared. MICS 542.12(c)(12)

D. At least three parts of each credit slip shall be utilized as follows: MICS 542.12(c)(13)

1. One part shall be retained in the cage for reconciliation of the cashier bank once signed by all participants and returned to the Cage with the credit;
2. Two parts shall be transported to the pit by the Security Department

member who transports chips, tokens, or monetary equivalents from the pit to the cage, and after the appropriate signatures are obtained, one part shall be deposited in the table drop box with the credit request duplicate;

3. One part shall be retained by the locked machine intact in a continuous unbroken form. PROVIDED, for an automated system, the restricted copy may be retained within the automated system.

E. The game, table number, shift, and the amount of credit by denomination and in total shall be noted on all copies of the credit slip. The correct date and time shall be indicated on at least two copies. MICS 542.12(c)(14)

F. Chips, tokens, and/or monetary equivalents shall be removed from the table tray by the dealer and shall be broken down or verified by the dealer in public view prior to placing them in racks for transfer to the cage. MICS 542.12(c)(15)

G. All chips, tokens, and monetary equivalents removed from the tables shall be carried to the cashier's cage by a Security Department member. MICS 542.12(c)(16); TSC App. A:17(7)(a)

H. The credit slip shall be signed by at least the following individuals (as an indication that each has counted the items transferred): MICS 542.12(c)(17); TSC App. A:17(5)

1. Cashier who received the items transferred from the pit and prepared the credit slip;
2. Security Department member who carried the items transferred from the pit to the cage and returned to the pit with the credit slip;
3. Dealer who had custody of the items prior to transfer to the cage; and
4. Gaming facility supervisor who supervised the credit transaction.

I. The credit slip shall be inserted with the credit request duplicate in the drop box by the dealer. MICS 542.12(c)(18)

J. Chips, tokens, or other monetary equivalents shall be deposited on or removed from gaming tables only when accompanied by the appropriate fill/credit slip. MICS 542.12(c)(19)

## 7.8. Table Games Computer Generated Documentation Standards

A. A computerized system may replace the manual fill or Credit process. TSC App. A:17(9)

1. The system is approved by the Tribal Gaming Agency prior to use after confirming the system meets the standards of control set out in the manual system
2. The system provides for adequate separation of duties within the system through passwords or other security features

3. If at any time the computerized system fails, the manual process will be followed until the computerized system returns to full capabilities

B. The computer system shall be capable of generating adequate documentation of all information recorded on the source documents and transaction detail (e.g., fill/credit slips, etc.). MICS 542.12(e)(1)

C. This documentation shall be restricted to authorized personnel. MICS 542.12(e)(2)

D. The documentation shall include, at a minimum, system exception information (e.g., appropriate system parameter information, corrections, voids, etc.). MICS 542.12(e)(3)(i)

E. The electronic system must include a personnel access listing, which includes, at a minimum: MICS 542.12(e)(3)(ii)

1. Employee name;
2. Employee identification number; and
3. Listing of functions employees can perform or equivalent means of identifying the same.

## 7.9. Playing Cards and Dice Standards

A. Playing cards and dice not yet issued to the pit shall be physically controlled by the Security Department and maintained in a secure location to prevent unauthorized access and reduce the possibility of tampering. MICS 542.12(f)(1); TSC App. A:6(3)(a)(iv)

B. Used cards and dice, when removed from play, shall be "marked," "scored," or "cancelled" to prevent unauthorized access and reduce the possibility of tampering. MICS 542.12(f)(3)

C. The Security Department shall physically control and maintain used playing cards and dice in a secure location until destroyed in a timely manner not to exceed seven days. However, this standard shall not apply where playing cards or dice are retained for an investigation. MICS 542.12(f)(3)

D. Card control logs shall be maintained that document when cards and dice are received on site, distributed to and returned from tables, or removed from play by the gaming operation, and destroyed. MICS 542.12(f)(4)

E. If a gaming operation uses plastic cards (not plastic-coated cards), the cards may be used for up to three (3) months if the plastic cards are routinely inspected, and washed or cleaned in a manner and time frame approved by TGA. MICS 542.12(g)

## 7.10. Analysis of Table Game Performance Standards MICS 542.12(i); TSC App. A:4(4)(a)

A. Records shall be maintained, by day and shift, indicating any single-deck blackjack games that were dealt for an entire shift.

B. Records reflecting hold percentage by table and type of game shall be maintained by shift, by day, cumulative month-to-date, and cumulative year-to-date.

C. This information shall be presented to and reviewed by management independent of the pit department on at least a monthly basis.

1. Such management shall investigate any unusual fluctuations in hold percentage with pit supervisory personnel.
2. The results of such investigations shall be documented, maintained for inspection, and provided to TGA upon request.

# Chapter 8 ELECTRONIC GAMING SYSTEMS

## 8.1. System Overview

A. The Electronic Gaming System (EGS) consists of both Class II and Class III gaming systems. Gaming Machine also consists of both Class II and Class III for the purposes of this control. The Tribal Lottery System (TLS) is a class III system with terminals referred to as Player Terminals. The bingo-based gaming system (BGS) is Class II with video terminals referred to as Electronic Gaming Machines (EGM) for the purposes of this control.

## 8.2. EGS Jackpot Standards

A. Jackpot Payouts and Accumulated Credit Payouts Standards for EGM/Player Terminal for jackpot payouts, documentation shall include the following information:

1. Date and time; (MICS 542.13(d)(i))
2. Machine number; (MICS 542.13(d)(ii))
3. Dollar amount of cash payout (both alpha and numeric) or description of personal property awarded, including fair market value. Alpha is optional if another unalterable method is used for evidencing the amount of the payout; (MICS 542.13(d)(iii))
4. Game outcome (including reel symbols, card values, suits, etc.) for jackpot payouts. Game outcome is not required if a computerized jackpot/fill system is used; (MICS 542.13(d)(iv))
5. Signatures of at least two employees verifying and witnessing the payout; (MICS 542.13(d)(vi))
6. Preprinted or concurrently printed sequential number. (MICS 542.13(d)(v))

B. Surveillance is notified prior to initiation of payout procedures for jackpot awards equal to or greater than $10,000

C. Jackpot payouts over $25,000 shall require the signature and verification of a supervisory or management employee independent of the Electronic Gaming Department (in addition to the two signatures required in paragraph 8.2.A.5 of this section). Alternatively, if an on-line accounting system is utilized, only two signatures are required: one employee and one supervisory or management employee independent of the Electronic Gaming Department. This predetermined amount shall be authorized by management (as approved by the Tribal gaming regulatory authority), documented, and maintained. (MICS 542.(d)(vi)(A)

D. Computerized jackpot systems shall be restricted so as to prevent unauthorized access and fraudulent payouts by one individual. (MICS 542.13(d)(3))

E. Payout forms shall be controlled and routed in a manner that precludes any one individual from producing a fraudulent payout and misappropriating the funds by forging signatures or by altering the amount paid out. (MICS 542.13(d)(4))

## 8.3. EGS Funds Standards

A. The Gaming Machine cage and change banks, which are active during the shift, shall be counted down and reconciled each shift utilizing a count sheet that documents funds by denomination. (MICS 542.13(f)(1))

## 8.4. EGM/Player Terminal Software Media Standards

A. At least annually, procedures shall be performed to insure the integrity of a sample of game software media by personnel independent of the gaming operation or the machines being tested. (MICS 542.13(g)(1))

B. Game software media control standards.

1. Procedures shall be developed and implemented for the following:

C. Removal of game software media, from devices, for verification or signature; (MICS 542.13(g)(2)(i))

1. Receipt and destruction of game software media; (MICS 542.13(g)(2)(iv)) and
2. Securing the game software media, from unrestricted access. (MICS 542.13(g)(2)(v))
3. Records, which document the above game software media procedures, shall include the following information:
   a) Date; (MICS 542.13(g)(5)(i))
   b) Machine number (source and destination); (MICS 542.13(g)(5)(ii))
   c) Manufacturer; (MICS 542.13(g)(5)(iii))
   d) Program number; (MICS 542.13(g)(5)(iv))
   e) Personnel involved; (MICS 542.13(g)(5)(v))
   f) Disposition of any permanently removed game software media; (MICS 542.13(g)(5)(vii))
   g) Approved testing lab approval numbers, if available. (MICS 542.13(g)(5)(ix))
4. The master game program number, par percentage, and the pay table shall be verified to the par sheet when initially received from the manufacturer. (MICS 542.13(g)(3))
5. EGM/Player Terminals shall have the circuit boards locked and the key(s) will be controlled by TGA. The lock shall necessitate the presence of an individual independent of the electronic game department to access the device game program game software media. (MICS 542.13(g)(4)

D. Game software media, returned to gaming devices shall be labeled with the program number. Supporting documentation shall include the date, program number, information identical to that shown on the manufacturer's label, and initials of the person replacing the game software media. (MICS 542.13(g)(6)

## 8.5. EGS Player Tracking

A. Systems shall be permissible that allow player tracking, maintenance tracking, and other gaming management or marketing functions. These systems shall not interfere with, or in any way affect, the outcome of any Tribal Lottery Game or the cashless accounting system. Systems shall be permissible that allow progressive prize management with the certification of the Gaming Test Laboratory and approval of the SGA. (TSC X2 8.3)

## 8.6. EGS Theoretical and Actual Hold Percentage Evaluation Standards

A. Accurate and current theoretical hold worksheets shall be maintained for each Gaming Machine. (MICS 542.13(h)(1))

B. Records shall be maintained for each machine which indicate the date the machine was placed into service, the date the machine was removed from operation, the date the machine was placed back into operation, and any changes in machine numbers and designations. (MICS 542.13(h)(7))

C. All of the Gaming Machines shall contain functioning meters which shall record credit-in. (MICS 542.13(h)(8))

D. All Gaming Machines with bill/ticket acceptors shall contain functioning ticket-in meters which record the value amounts or number of bills/tickets accepted. (MICS 542.13(h)(9))

E. GamingGaming Machine in-meter readings shall be recorded at least weekly immediately prior to or subsequent to a Gaming Machine drop. However, the time between readings may extend beyond one week in order for a reading to coincide with the end of an accounting period only if such extension is for no longer than six days. (MICS 542.13(h)(10))

F. The employee who records the in-meter reading shall either be independent of the count team or shall be assigned on a rotating basis, unless the in-meter readings are randomly verified quarterly for all Gaming Machines and currency acceptors by someone other than the regular in-meter reader. (MICS 542.13(h)(11))

G. Upon receipt of the meter reading summary, the accounting department shall review all meter readings for reasonableness using pre-established parameters. (MICS 542.13(h)(12))

H. Prior to final preparation of statistical reports, meter readings that do not appear reasonable shall be reviewed with Electronic Gaming Department employees, and exceptions documented, so that meters can be repaired or clerical errors in the recording of meter readings can be corrected. (MICS 542.13(h)(13))

I. A report shall be produced at least monthly showing month-to-date, year-to-date, and if practicable, life-to-date actual hold percentage computations for individual machines and a comparison to each machine's theoretical hold percentage previously discussed. (MICS 542.13(h)(14))

J. Each change to a Gaming Machine's theoretical hold percentage, including progressive percentage contributions, shall result in that machine being treated as a new machine in the statistical reports (i.e., not commingling various hold percentages). (MICS 542.13(h)(15))

K. If promotional payouts or awards are included on the Gaming Machine statistical reports, it shall be in a manner that prevents distorting the actual hold percentages of the affected machines. (MICS 542.13(h)(16))

L. The statistical reports shall be reviewed by both Electronic Gaming Department management and management employees independent of the Electronic Gaming Department on at least a monthly basis. (MICS 542.13(h)(17))

M. those machines that have experienced at least 100,000 wagering transactions, Large variances (three percent (3%) recommended) between theoretical hold and actual hold shall be investigated and resolved by a department independent of the Electronic Gaming Department with the findings documented and provided to the TGA upon request in a timely manner. (MICS 542.13(h)(18))

N. TGA will be notified and follow-up shall be performed for any one machine having an unresolved variance between actual cash drop and the report information in excess of an amount that is both more than $25 and at least three percent (3%) of the actual cash drop. The follow-up performed and results of the investigation shall be documented and maintained for inspection. (MICS 542.13(m)(5)(7))

O. Maintenance of the computerized Gaming Machine monitoring system data files (if applicable) shall be performed by a department independent of the Electronic Gaming Department. Alternatively, maintenance may be performed by gaming machine supervisory employees if sufficient documentation is generated and it is randomly verified on a monthly basis by employees independent of the Electronic Gaming Department. (MICS 542.13(h)(19))

P. Updates to the computerized Gaming Machine monitoring system (if applicable) to reflect additions, deletions, or movements of Gaming Machines shall be made at least weekly prior to in- meter readings. (MICS 542.13(h)(20))

## 8.7. In-house Progressive EGS Standards

A. A meter that shows the amount of the progressive jackpot shall be conspicuously displayed at or near the machines to which the jackpot applies. (MICS 542.13(k)(1)) At least once a month, each gaming operation shall record the amount shown on each progressive jackpot meter at the gaming operation except for those jackpots that can be paid directly from the machine; (MICS 542.13(k)(2))

B. Explanations for meter reading decreases shall be maintained with the progressive meter reading sheets, and where the payment of a jackpot is the explanation for a decrease, the gaming operation shall record the jackpot payout number on the sheet or have the number reasonably available; and (MICS 542.13(k)(3))

C. Each gaming operation shall record the base amount of each progressive jackpot the gaming operation offers. (MICS 542.13(k)(4))

D. The TGA shall approve procedures specific to the transfer of progressive amounts in excess of the base amount to other Gaming Machines. Such procedures may also include other methods of distribution that accrue to the benefit of the gaming public via an award or prize. (MICS 542.13(k)(5))

## 8.8. EGM Wide Area Progressive Standards

A. A meter that shows the amount of the progressive jackpot shall be conspicuously displayed at or near the machines to which the jackpot applies. (MICS 542.13(l)(1))

B. As applicable to participating gaming operations, the wide area progressive Gaming Machine system shall be adequately restricted to prevent unauthorized access. (MICS 542.13(l)(2))

C. The TGA shall approve procedures for the wide area progressive system that: (MICS 542.13(l)(3))

1. Reconcile meters and jackpot payouts;
2. Collect/drop Gaming Machine funds;
3. Verify jackpot, payment, and billing to gaming operations on pro-rata basis;
4. System maintenance;
5. System accuracy; and
6. System security.

## 8.9. EGS Cash-Out Ticket Standards

A. For EGS machines that accept currency (or tickets) and issue cash-out tickets, the following standards shall apply:

1. In addition to the applicable portions of Electronic Game Accounting/Auditing Procedures Standards, on a quarterly basis, the gaming operation shall foot all jackpot cash-out tickets and trace totals to those produced by the system. (MICS 542.13(n)(1)
2. The customer may request a cash-out ticket from the EGM/Player Terminal that reflects all remaining credits. The cash-out ticket shall be printed at the EGM/Player Terminal by an internal document printer. (MICS 542.13(n)(2)
3. The customer shall redeem the cash-out ticket at a cashier's cage or redemption kiosk. (MICS 542.13(n)(3) Once presented for redemption, the cashier shall:
    a) Scan the bar code via an optical reader or its equivalent; or (MICS 542.13(n)(4)(i)
    b) Input the cash-out ticket validation number into the computer. (MICS 542.13(n)(4)(ii)
4. Alternatively, if operation utilizes a remote computer validation system, operation as approved by TGA, shall develop alternate standards for the maximum amount that can be redeemed, which shall not exceed $2,999.99 per cash-out transaction. (MICS 542.13(n)(3)
5. The information from the cash-out ticket presented shall be transmitted to the host computer. The host computer shall verify the authenticity of the cash-out ticket and communicate directly to the cashier cage terminal. (MICS 542.13(n)(5)
6. If valid, the cashier pays the customer the appropriate amount and the cash-out ticket is electronically noted "paid" in the system. The "paid" cash-out ticket shall remain in the cashier's bank for reconciliation purposes. (MICS 542.13(n)(6)
7. If invalid, the host computer shall notify the cashier that one of the following conditions exists: (MICS 542.13(n)(7)
    a) The serial number cannot be found on file (stale date, forgery, etc.);
    b) The cash-out ticket has already been paid; or
    c) The amount of the cash-out ticket differs from the amount on file.
8. If invalid, the cashier shall refuse payment to the customer and notify a supervisor of the invalid condition. The supervisor shall resolve the dispute. (MICS 542.13(n)(7)
9. If the host validation system temporarily goes down, cashiers may

redeem cash-out tickets after recording the following: (MICS 542.13(n)(8)

a) Serial number of the cash-out ticket;

b) Date and time;

c) Dollar amount;

d) Issuing EGM/Player Terminal number;

e) Mark the ticket as “paid”; and

f) Ticket shall remain in cashier's bank for reconciliation purposes.

10. Such cash-out tickets redeemed shall be validated as expeditiously as possible when the cashless electronic game system is restored. (MICS 542.13(n)(9)

11. The operation shall develop and implement procedures to control cash-out ticket paper which shall include procedures which: (MICS 542.13(n)(10)

a) Mitigate the risk of counterfeiting of cash-out ticket paper;

b) Adequately controls the inventory of the cash-out ticket paper; and

c) Provide for the destruction of all unused cash-out ticket paper.

12. If the host validation system is down for more than one hour, the gaming operation shall promptly notify TGA. (MICS 542.13(n)(11)

## 8.10. EGS Kiosks

A. Kiosks shall have reports that properly document all transactions, as well as dedicated video surveillance, to protect the integrity of the cashless system used. Cash boxes shall be designed so their contents are protected from unauthorized access, in accordance with Appendix A drop box and transportation standards and shall be uniquely labeled for the purpose of audit and security. (TSC X2 8.4)

## 8.11. Description of Tribal Lottery System (TLS) General Description (TSC X2 3.1):

A. The Tribal Lottery System game known as the Electronic Scratch Ticket Game consists of a finite number of Electronic Scratch Tickets, a certain number of which, if drawn, entitle a player to prize awards at various levels. The scratch tickets are designed from a template in conformity with this Appendix and are created in Game Sets on a Manufacturing Computer from which Scratch Tickets are randomly selected and placed into Scratch Ticket Subsets. Each Game Set has a predetermined number of winners and values and is designed so as to assure players of an at least 75% payback of the amounts paid in the aggregate for all tickets in the Set. As a Game Set’s tickets are placed into Subsets, the pool of tickets available from that Game Set for placement into Subsets diminishes, until each ticket in the Game Set has been placed into a Subset. (TSC X2 3.1.1)

B. Scratch Ticket Subsets are transmitted to the Central Computer, where they are stored until dispensed electronically on demand to Player Terminals. Scratch Tickets are electronically dispensed from the Central Computer in the order within each Subset in which the tickets were received. Players compete against each other to draw winning tickets. As Subsets are used they are replaced by additional Subsets which have been created and delivered to the Central Computer in the same manner, until the Game Set has been depleted, or pulled from play, ending that particular game. Different games based on different Game Sets may be offered simultaneously through the Central Computer. (TSC X2 3.1.2)

C. A player initiates participation in an Electronic Scratch Ticket game at a Player Terminal, using Game Play Credits purchased on the Player Terminal through the insertion of cash, or through the Cashless Transaction System. The monitor displays one or more of the Electronic Scratch Ticket games that are offered by the system, as well as other information such as graphics, game play and outcome information, and entertainment effects, subject to the limitations in Sections 5.2.2 and 5.2.3. The player may choose a particular game and reveal the outcome, by touching the screen, pressing a button once or performing some other form of interaction with the Player Terminal. (TSC X2 3.1.3)

1. Following or as part of the player's selection of a game or games, the player uses Game Play Credits displayed on the Player Terminal to purchase one or more Electronic Scratch Tickets. The pricing of tickets is governed by the provisions of Section 8.13. Wagers are deducted from the Game Play Credits displayed on the Player Terminal. (TSC X2 3.1.4)
2. Prize structure, ticket purchase and selection, and wager information is displayed or available on the Player Terminal with respect to any game which is being played through that Terminal. (TSC X2 3.1.5)
3. After the player purchases an Electronic Scratch Ticket the outcome associated with that ticket is shown on the Player Terminal. Any prizes won are displayed on the Player Terminal and may be in the form of Game Play Credits, the right to receive merchandise, or other valuable property. (TSC X2 3.1.6)
4. Game Play Credits earned as prizes remain displayed and available for use in further play from that Terminal. Game Play Credits also may be electronically transferred to a) a player's account in the Central Accounting System, b) a ticket or receipt printed by the Player Terminal, or c) a "smart" card or similar instrument. Once transferred, Game Play Credits may be a) used for further play on another Terminal or b) redeemed for cash or cash equivalents through a cashier or other separate redemption system. Merchandise or other property won is collected in accordance with the rules of the game. (TSC X2 3.1.7)

## 8.12. Ticket Lottery System (TLS)TLS Cashless Transaction Security, Reporting and Storage Requirements

A. The following requirements shall be met in connection with any Cashless Transaction System: (TSC X2 8.1)

B. All player information must be stored on at least two separate non-volatile media; (TSC X2 8.1.1)

C. An audit file must be kept of all player financial transactions. This file must be stored in at least two separate non-volatile media, and be accessible for purposes of audit and dispute resolution to authorized individuals; this file must be available on-line for a minimum of 30 days, after which it must be available off line for a minimum of 180 days; (TSC X2 8.1.2)

D. Physical and operational controls must be used to protect player information from tampering or unauthorized access; (TSC X2 8.1.3)

E. Passwords or personal identification numbers (PINs), if used, must be protected from unauthorized access; (TSC X2 8.1.4)

F. All player information shall be accurately recorded and such recording protected by the system; (TSC X2 8.1.6)

G. Any card or other tangible instrument issued to a player for the purpose of using the Cashless Transaction System shall bear on its face a control or inventory number unique to that instrument; (TSC X2 8.1.7)

H. Encoded bearer instruments printed or magnetic may include coupons and other items distributed or sold for game play, promotional, advertising or other purposes, but may not include cash. Such instruments must be in electronically readable form in addition to having unique identification information printed on the instrument face. The daily and monthly reporting must include with respect to such instruments:

1. Cash converted to value in the cashless system
2. Outstanding unredeemed balance:
3. Value in the cashless system converted to cash;
4. Amount wagered; and
5. Amount won. (TSC X2 8.1.8)

I. Redemption periods, if any, shall be posted or otherwise disclosed to all players. (TSC X2 8.1.9)

J. Vouchers must bear on the face, in addition to the unique serial number, the following:

1. Time/Date printed;

2. Unique identification from which it was printed; and
3. Value of voucher. (TSC X2 8.1.10)

## 8.13. TLS Game Set and Subset Requirements (TSC X2 3.2) Each Game Set shall meet the following minimum requirements:

A. Each Game Set shall be made up of a finite number of Electronic Scratch Tickets;

B. All Scratch Tickets in a particular Game Set shall be of the same purchase price, which shall not exceed $5.00, with the exception that up to 15 percent of the Player Terminals in operation may have purchase prices of up to $20.00 per Ticket. A single Ticket may offer an opportunity to enter another Game Set;

C. The payout percentage for the entire Game Set shall be no less than 75% of the total purchase price of all tickets in the set combined;

D. Each Game Set shall be assigned a unique serial number; and

E. Each ticket shall have a specific outcome and prize level associated with it. (TSC X2 3.2.1)

## 8.14. TLS Game Set Verification Process.

A. Prior to commencement of play, the initial Game Set shall be verified as to the total number of tickets in the set and the number of winners at each prize level, including the amounts of such prizes, and the number of non-winners. The verification standards which the Game Set must meet are those set forth in Section 8.18. (TSC X2 3.2.2)

## 8.15. TLS Transmission of Subsets to Central Computer.

A. Following verification of the Game Set, the Manufacturing Computer shall create ordered Scratch Ticket Subsets on demand from the Central Computer and transmit the ordered Subsets to it. (TSC X2 3.2.3)

## 8.16. TLS Subset Requirements.

A. Each Electronic Scratch Ticket Game Subset shall meet the following minimum requirements:

1. Within a given Game Set, each Subset shall be the same size and comprised of no less than 5,000, and no more than 10,000 Electronic Scratch Tickets, provided that in order to complete the distribution of all tickets in a Game Set, the final Subset derived from the Set may have less than the number of tickets in any other Subset and be less than 5,000;
2. Each Subset shall be individually and uniquely identified by the Game Set serial number and a unique serial number for each Subset assigned in the order in which the Subsets are created;

3. Once an Electronic Scratch Ticket has been dispensed to a Player Terminal from a Subset, it cannot be dispensed again. (TSC X2 3.2.4)

## 8.17. TLS Completion of Game.

A. A Scratch Ticket Game is deemed to be completed only when all of the Electronic Scratch Tickets in a Game Set have been dispensed or the Game Set has been taken out of play. If any Game Set is withdrawn from play before completion of the Game, the Tribe shall ensure that at least 75% of the revenues received from sales of Electronic Scratch Tickets in that Game have been, or in future Electronic Scratch Ticket Games will be, awarded to players. (TSC X2 3.2.5)

## 8.18. TLS Data Required Prior to Commencement of an Electronic Scratch Ticket Game.

A. The following data shall be available to the TGA and SGA prior to the commencement of an Electronic Scratch Ticket Game and shall be maintained and be viewable both electronically and if requested, by printed report, upon demand: (TSC X2 3.3)

1. A unique identifying Game Set serial number; (TSC X2 3.3.1)
2. A description of the Game Set theme sufficient to categorize the Game Set relative to other Game Sets; (TSC X2 3.3.2)
3. The number of total Scratch Tickets in the Game Set; (TSC X2 3.3.3)
4. The number of Scratch Ticket Subsets to be created from the Game Set, and the number of tickets in each Set; (TSC X2 3.3.4)
5. The payout percentage of the entire Game Set; (TSC X2 3.3.5)
6. The payout table for the Game Set and the number of Scratch Tickets at each level of the payout table; (TSC X2 3.3.6)
7. The purchase price per ticket assigned to the Game Set; (TSC X2 3.3.7)
8. Such further information as the SGA may reasonably require to assure the integrity and accuracy of the foregoing information. (TSC X2 3.3.8)

## 8.19. TLS Data Required to be Available Following the Completion of a Scratch Ticket Game.

A. Following the completion of an Electronic Scratch Ticket Game (i.e., upon the sale of all tickets in a Game Set or the withdrawal of the Set from play), the following data shall be available to the TGA and SGA and shall be maintained and viewable both electronically and if requested, by printed report, upon demand: (TSC X2 3.4)

1. The Game Set and Game Subsets serial numbers; (TSC X2 3.4.1)
2. The total number of Electronic Scratch Tickets unsold, if the game is removed from play; (TSC X2 3.4.2)

3. The total number of Electronic Scratch Tickets purchased; (TSC X2 3.4.3)
4. The time and date that each Subset was transmitted to the Central Computer; (TSC X2 3.4.4)
5. The time and date that the game was completed or removed from play; (TSC X2 3.4.5)
6. The final payout percentage of the game; and (TSC X2 3.4.6)
7. Price per Ticket. (TSC X2 3.4.7)

## 8.20. TLS Software Auditing Tool to be Made Available.

A. For auditing Game Sets and Subsets that have been archived, any Tribal Lottery System shall include and have available for the SGA and the TGA a secure software tool which provides the same data as set forth in Section 8.18 and 8.19, provided that such tool shall be used only during authorized audits of Tribal Lottery System games and operations, or in cases of player disputes, and shall not be used for any other purpose without the consent of the TGA and the SGA. (TSC X2 3.5)

## 8.21. TLS No Audit of Set While in Play; Dispute Process

A. No Audit of Set While in Play In order to provide maximum game integrity, no audit or other determination of the status of any Game Set or any Subset, including but not limited to a determination of the prizes won or prizes remaining to be won, shall be conducted by anyone, including TGA and SGA personnel, while a Subset is in play without causing termination of the entire Game Set from which the Subset was derived as provided in paragraph C of this section. (TSC X2 3.6.1)

B. Dispute Resolution: Impact on Game Set Play. In the event of a dispute by a player that cannot be resolved by ordinary means by Gaming Facility personnel as to the outcome, prize, wager made, or any other aspect of the player's participation in a Game Set being played, all relevant data shall be immediately collected, including but not limited to all meter readings, memory records, surveillance recordings, and any other reports or information regarding play at the Terminal for the play in dispute. Following the collection of all relevant data, the TGA shall be notified and requested to make an evaluation of whether or not the dispute involves the integrity of the hardware or software being used and to try and resolve the dispute. A report of all disputes shall be maintained by the TGA. If the dispute is not resolved within 72 hours from the time of the complaint, the TGA shall immediately forward a report to the SGA detailing the nature of the dispute. In the event the dispute is resolved, the TGA is not obligated to report to the SGA, but shall make TGA reports available for review. (TSC X2 3.6.2)

C. Termination of Game Set. Protection of game integrity, even if it requires the early withdrawal of a Game Set from play, shall be the primary goal of this

Appendix. If resolution of a patron dispute requires access to data or records stored on any part of a system other than the Player Terminal involved in the dispute, and such access can only be accomplished through a means by which data would be revealed that could materially assist anyone in determining the likelihood of a particular ticket being drawn, other than information available to all patrons, the Game Set shall be terminated prior to accessing such data or records. (TSC X2 3.6.3)

D. TGA/SGA Disputes. In the event there is a dispute between the TGA and SGA at any point in the above process, it shall be resolved in accordance with the dispute resolution process for such issues set forth in the Compact. (TSC X2 3.6.4)

## 8.22. TLS Manufacturing Computer (TSC X2 3.7)

A. Security from Alteration, Tampering, or Unauthorized Access. The Manufacturing Computer shall provide a physical and electronic means, by use of a password or other method approved by the TGA and SGA, for securing the Game Set against alteration, tampering, or unauthorized access. The Manufacturing Computer shall provide a means for terminating the Game Set if unopened ticket information from an operating Game Set or Subset has been accessed except as permitted in this Appendix. The Gaming Test Laboratory shall certify that such security system, and a means for monitoring its use in accordance with this Appendix, is included in the system before it may be authorized for use. Security systems and monitoring may be required for any component that has electronic access to this system that may violate the integrity and security of the manufacturing computer. (TSC X2 3.7.1)

B. Primary Purpose; Separation. The Manufacturing Computer shall be dedicated primarily to those Tribal Electronic Scratch Ticket gaming system functions related to the creation of Scratch Ticket Game Sets and the creation, randomization, and transmittal to the Central Computer of Scratch Ticket Subsets. Notwithstanding the foregoing, the Manufacturing Computer may also be used for other computer functions in the Tribal Lottery System or Electronic Accounting System if such use will not affect the integrity or outcome of any game. (TSC X2 3.7.2)

C. Storage Medium; Backup. The Manufacturing Computer shall have a medium for securely storing Electronic Scratch Ticket Game Sets and Subsets on the Manufacturing Computer which shall be mirrored on line by a backup medium within the same cabinet or enclosure. In addition, duplicates of the Sets and Subsets, as created and stored on the Manufacturing Computer, shall be stored in a secure enclosure in the Gaming Facility separate from the Manufacturing Computer. All storage shall be through an error checking, nonvolatile physical medium, so that should the primary storage medium fail, there will be no critical data loss. (TSC X2 3.7.3)

D. Randomization. The Manufacturing Computer shall utilize randomizing procedures in the creation of the Subsets. The randomizing procedures shall be in accordance with Section 6 of this Appendix. (TSC X2 3.7.4)

## 8.23. TLS Central Computer Used in Connection with Electronic Scratch Ticket Game.

A. The following requirements apply to any Central Computer used in connection with an Electronic Scratch Ticket Game. (TSC X2 3.8)

1. Dispensing of Tickets. The Central Computer shall dispense, upon request from a Player Terminal, Electronic Scratch Tickets. (TSC X2 3.8.1)
2. Order of Scratch Tickets. The Central Computer shall maintain Electronic Scratch Ticket Subsets in the order received from the Manufacturing Computer, and transmit them in that order to Player Terminals on demand, provided that not less than two (2) nor more than five (5) Subsets per Game Set shall be dispensed in accordance with a predetermined order for rotating the Subsets. Subsets from more than one Game Set may be stored on the Central Computer and made available for play at the same time. (TSC X2 3.8.2)
3. Storage Medium; Backup. The Central Computer shall have a medium for storing Electronic Scratch Ticket Game Subsets and reflecting their current status of play, which shall be mirrored on line by a backup medium within the same cabinet or enclosure. All storage shall be through an error checking, nonvolatile physical medium, so that should the primary storage medium fail, there will be no critical data loss. (TSC X2 3.8.3)
4. No Randomization Capability. The Central Computer shall have no randomization capability associated with its use in an Electronic Scratch Ticket game. (TSC X2 3.8.4)

## 8.24. TLS Data Available for Inspection.

A. The following data is required to be available for inspection in compliance with Appendix X2, Section 7.1.9 for any Player Terminal or Game Set: (TSC X2 3.10)

1. All Game Set serial numbers, indicating the date and time the Game Set was put in play, pulled from play, or completed. (TSC X2 3.10.1)
2. By Game Set serial numbers, the Player Terminal numbers assigned, and the dates and times of assignment to the Player Terminals. (TSC X2 3.10.2)

## 8.25. Player Terminals.

All Player Terminals shall conform at a minimum to the requirements of this Section.

A. Use as a Stand-Alone Gambling Device Prohibited. No Player Terminal shall be capable of being used as a stand-alone unit for the purposes of engaging in any gambling game, including but not limited to the lottery games described in this Compact, or in any other way prohibited in this Appendix. (TSC X2 5.1)

B. Player Terminals shall include the following features:

1. Operation either through the Cashless Transaction System, or through means for accepting cash (coins, tokens or paper currency) for conversion into Game Play Credits, which can then activate participation in the game, provided the insertion of cash will not alone activate the game and such use of cash is in accordance with Section 8.29; (TSC X2 5.2.1)
2. One or more of the following: A video monitor, electro-mechanical display, printer, graphics and signage, provided that slot machine-type spinning reel mechanisms are prohibited in mechanical form; and (TSC X2 5.2.2)
3. One or more of the following: electronic buttons, touch screen capability, and a mechanical, electro-mechanical or electronic means of activating the game and providing player input, including a means for making player selections and choices in games, provided that slot machine type handles are prohibited. (TSC X2 5.2.3)

C. Non volatile backup memory or its equivalent shall be maintained in a secure compartment on each Player Terminal for the purpose of storing and preserving a redundant set of critical data which has been error checked in accordance with this Appendix, and which data shall include, at a minimum, the following Player Terminal information: (TSC X2 5.3)

1. Recall of all wagers and other information associated with the last ten (10) Electronic Scratch Ticket plays and the last ten (10) On-line Lottery Games played; (TSC X2 5.3.2)
2. Error conditions that may have occurred on the Player Terminal; and (TSC X2 5.3.3)
3. Recall of the last twenty five (25) cash or cash equivalent deposits. (TSC X2 5.3.4)

D. An on/off switch that controls the electrical current that supplies power to the Player Terminal must be located in a secure place that is readily accessible within the interior of the Player Terminal.

E. The operation of each Player Terminal must not be adversely compromised or affected by static discharge, liquid spills, or electromagnetic interference. (TSC X2 5.5)

F. A Player Terminal must have electronic accounting meters which have tally totals to a minimum of eight (8) digits and be capable of rolling over when the maximum value of at least 99,999,999 is reached. The Player Terminal must

provide a means for on-demand display of the electronic meters via a key switch or other secure method on the exterior of the machine. Electronic meters on each Player Terminal for each of the following data categories for Electronic Scratch Ticket games and On-line Lottery Games are required in compliance with Appendix Xw2, Section 7.1.9: (TSC X2 5.6)

1. Credits, or equivalent monetary units, wagered on a cumulative basis on that Terminal; (TSC X2 5.6.1)
2. Credits, or equivalent monetary units, won for the Player Terminal; (TSC X2 5.6.2)
3. For Scratch Ticket games, the number of Scratch Tickets purchased on the Terminal; and (TSC X2 5.6.3)
4. For On-line Lottery games, the number of On-line Lottery wagers made on that Terminal. (TSC X2 5.6.4)

G. Under no circumstances shall the Player Terminal electronic accounting meters be capable of being automatically reset or cleared, whether due to an error in any aspect of its or a game's operation or otherwise. All meter readings must be recorded and dated in the presence of a TGA inspector both before and after an electronic accounting meter is cleared. (TSC X2 5.7)

H. At a minimum, each Player Terminal shall have the following game information available for display on the video screen and/or displayed on the Player Terminal itself, in a location conspicuous to the player: (TSC X2 5.8)

1. The rules of the game being played; (TSC X2 5.8.1)
2. The maximum and minimum wagers and the amount of credits, cash equivalents, or additional game play opportunities, which may be won for each Electronic Scratch Ticket and On-line Lottery Game offered through that Terminal, including the current values of any progressive prizes available; (TSC X2 5.8.2)
3. The player's credit balance; (TSC X2 5.8.3)
4. The outcome of the Electronic Scratch Ticket(s) then being played; and (TSC X2 5.8.4)
5. Any prize won on the Electronic Scratch Ticket(s) then being played. (TSC X2 5.8.5)

I. The video screen or other means for displaying game rules, outcomes and other game information shall be kept under a glass or other transparent substance which places a barrier between the player and the actual surface of the display. At no time may stickers or other removable media be placed on the Player Terminal's face for purposes of displaying rules or payouts. (TSC X2 5.9)

J. No hardware switches may be installed on a Player Terminal or any associated equipment which may affect the outcome or pay out of any game for which the Player Terminal is used. Switches may be installed to control the ergonomics of

the Player Terminal. (TSC X2 5.10)

K. The Player Terminal shall record the date and time of any opening of cabinet door(s); provided, that this information need not be retained on the Player Terminal if it is communicated to another component of the system. This information shall be retrievable in report form. (TSC X2 5.16)

L. Player Terminals shall not have software or hardware that determines the outcome of any Electronic Scratch Ticket Game. Nothing herein is intended to prohibit the Player Terminal from creating the appropriate Scratch Ticket and On-line Game graphics and animation to correspond to, display or represent, in an entertaining manner, the outcome. In addition, Player Terminals shall not have any software that: (TSC X2 5.12)

1. Determines which Scratch Ticket outcome from within the Scratch Ticket Subset is transmitted to the Player Terminal; or (TSC X2 5.12.1)
2. Alters the amount of the payout of the Electronic Scratch Ticket as received from the Central Computer. (TSC X2 5.12.2)

M. Nothing herein shall prohibit the use of a quick pick function on the Player Terminal in conjunction with the playing of the On-line Lottery Game. (TSC X2 5.13)

N. Players shall make wagers using a Player Terminal to purchase Electronic Scratch Tickets. Following a purchase, the Electronic Scratch Ticket shall be displayed on the Terminal's video screen for the purpose of revealing the outcome of the selected ticket. (TSC X2 5.14)

## 8.26. TLS Networking Requirements.

A. The use of firewalls and other system protections as approved by TGA and SGA are required to protect the integrity of the Tribal Lottery System and player accounts and: (TSC X2 5.11)

1. Where the Tribe's Tribal Lottery System or components are linked with one another in a local network for progressive jackpot, function sharing, aggregate prizes or other purposes, communication protocols must be used which ensure that erroneous data or signals will not adversely affect the operations of any such system or components. No class III game or gaming system in which any part or component is located outside the Tribe's gaming facilities shall be deemed approved as part of the approval of this Appendix. Any proposal for such game or gaming system, including the proposed rules, manner of regulation, and manner of play, monitoring and/or maintenance of the system, shall require submission to, and approval by, the TGA and SGA. (TSC X2 5.11.1)
2. Dedicated and protected network connections prohibiting unauthorized access, approved by SGA and TGA, may allow two or more of the Tribe's Tribal Lottery Systems to share player information. Game tickets and

other information prohibited from being viewed, as outlined in other sections of this Appendix, shall not be available or transmitted between the Tribe's connected Tribal Lottery Systems or facilities. Communications between the Tribe's facilities will require the use of approved firewalls that are configured and operated to protect the Tribal Lottery System and player information. Computer systems linked between the Tribe's facilities may not be used to link progressive jackpots, except in Joined Facilities. (TSC X2 5.11.2)

## 8.27. TLS Security Requirements.

A. The following requirements apply to all components of the Tribal Lottery System, including the Manufacturing Computer, the Central Computer, the Electronic Accounting System and Player Terminals. (TSC X2 9)

1. The Manufacturing Computer, Central Computer, and Player Terminals in each Tribal Lottery System shall be physically and operationally independent from one another except as specified otherwise in this Appendix, such as for communications, storage and security monitoring, including the routing of communications among system components, provided such routing does not affect the integrity of the communications or the outcome of any game. All Tribal Lottery System cables shall be secured against unauthorized access. (TSC X2 9.1)

   a) Live network jacks shall be locked to prevent someone from removing the legitimate connection and plugging in an unauthorized device.

   b) Network jacks and cables that are not being utilized will either be locked or physically disconnected from the network so they are no longer active.

2. The Manufacturing Computer and Central Computer must be in a locked, secure enclosure with both camera coverage and key controls in place. Routers, switches, hubs, or other network access points, to include management terminals and terminals not separated from the Tribal Lottery System by firewalls approved by the WSGC and TGA, must also be in a locked, secure enclosure with both camera coverage and key controls in place. Access to Manufacturing Computers and Central Computers shall be logged by the system to include the date and time of access and available to WSGC and TGA upon request. (TSC X2 9.2)

   a) The TLS remote workstation Central Processing Unit shall at a minimum be enclosed in a locked and monitored cabinet. Keys to the cabinet shall be maintained in accordance with the approved Tribal Operations Internal Controls.

   b) Remote workstations shall prevent access to the network or application based tools that allow access to restricted gaming

information. In addition, any account information access must follow approved internal controls.

3. Connections between all components of the Tribal Lottery System shall only be through the use of secure communication protocols which are designed to prevent unauthorized access or tampering, employing Data Encryption Standards (DES) or equivalent encryption with changeable seeds or algorithms. (TSC X2 9.3)

4. Each component of the Tribal Lottery System shall at all times be connected to a device which provides surge protection on any line that feeds it and, with the exception of Player Terminals, shall be connected to a temporary power source, such as a UPS, to provide means for an orderly shutdown of the computer in the event of a main power system failure. (TSC X2 9.4)

5. A non-removable plate shall be affixed to the exterior of each Player Terminal which shall have written upon it the Terminal's serial number and model number of the component and name of the manufacturer. Other audit numbers may be required to be affixed to provide a means of identifying individual Terminals for correlation to required reports. (TSC X2 9.5)

6. The Manufacturing and Central Computers shall at a minimum be enclosed in a locked and monitored cabinet. Access shall be through the use of access controls provided in paragraph 7 of this section. The Player Terminal shall have at a minimum the following separately locked areas, which shall be the only means of accessing any non-public part of the Terminal: (a) a locked and monitored cabinet door; (b) a locked microprocessor compartment; (c) a locked outer cash box door; and (d) a locked drop cash box door. (TSC X2 9.6)

7. Keys which provide access to any locked compartment, component or area of a Tribal Lottery System, as well as passwords, keycards, or PIN numbers used to access the Tribal Lottery System, shall be maintained and used in accordance with the access control standards enacted in the Tribe's statement of minimum internal controls. (TSC X2 9.7)

    a) Each employee accessing the Tribal Lottery System software except for Player Terminals and unattended Kiosks by means of a password, keycard, or PIN number, including vendor representatives, must have a user name or user number unique to that individual, and the Tribal Lottery System must log the date and time of access. These access logs must be readily available for audit by TGA and WSGC. (TSC X2 9.7.1)

8. For all entries into the locked areas of the Manufacturing Computer, Central Computer, unattended Kiosks, or any Player Terminal, a written record must be made on a machine entry authorization log (MEAL)

indicating at least the following: the time, date, and purpose of entering said locked area(s), and the name and employee number (or other personal identification specific to such person) of the person doing so. (TSC X2 9.8)

9. In addition to maintenance of MEAL cards, the Manufacturing and Central Computers shall record and generate a report on any access including date, time of access, person (by employee number) accessing the computer, and the reason for access. (TSC X2 9.9)

10. For purposes of this section, all components of the Tribal Lottery System, except wiring, cables, and conduit in which they are located, shall have the ability to be effectively and clandestinely monitored and recorded by means of a closed circuit television system or digital surveillance system in accordance with Appendix A and as authorized by TGA and SGA, in compliance with the requirements of the Compact. (TSC X2 9.10)

    a) Overhead camera coverage should be sufficient to identify the individual(s) accessing remote workstations. The coverage should not include the keyboard so sensitive passwords cannot be viewed and recorded. Coverage should be recorded real-time, full screen, and on dedicated VCR's or digital recorders.

11. In addition to its functions in operating a connection with the Electronic Scratch Ticket and On-line Lottery Games, the Central Computer may be used to record the data used to verify game play and to configure and perform security checks on Player Terminals, provided such functions do not affect the security, integrity or outcome of such games. (TSC X2 9.11)

    a) The TLS Manufacturing Computer shall provide a physical and electronic means, by use of a password or other method approved by the TGA and State Gaming Agency, for securing the Game Set against alteration, tampering, or unauthorized access. (TSC X2 9.7.1)

## 8.28. BGS & EGM Requirements

A. Controls must be established, and procedures implemented to safeguard the integrity of technological aids to the play of bingo during installations, operations, modifications, removal and retirements. Such procedures must include the following: (MICS 543.8(g)

1. Shipping and receiving MICS 543.8(g)(1)

    a) A communication procedure between the supplier, the gaming operation, and TGA to properly control the shipping and receiving of all software and hardware components, including: (MICS 543.8(g)(1)

        (1) Notification of pending shipments to be provided to the TGA by the gaming operation;

        (2) Certification in accordance with 25 CFR part 547;

(3) Notification from the supplier to the TGA, or the gaming operation as approved by the TGA, of the shipping date and expected date of delivery. The shipping notification must include:

(i) Name and address of the supplier;
(ii) Description of shipment;
(iii) For player interfaces: a serial number;
(iv) For software: software version and description of software;
(v) Method of shipment; and
(vi) Expected date of delivery.

b) Procedures for the exchange of the gaming system components for maintenance and replacement.

c) Procedures for shipping and receiving BGS components in a secure manner to deter unauthorized access.

d) TGA, or its designee, must receive all the gaming system components and game play software packages, and verify the contents against the shipping notification.

2. Security and access control methods. (MICS 543.8(g)(2)

a) Physical and operational controls must be established to restrict access to the gaming system components and protect player information from tampering or unauthorized access.

3. Recordkeeping and audit processes. (MICS 543.8(g)(3)

a) The gaming operation must maintain the following records, as applicable, related to installed game servers and player interfaces:

(1) Date placed into service;
(2) Date made available for play;
(3) Supplier;
(4) Software version;
(5) Serial number;
(6) Game title;
(7) Asset and/or location number;
(8) Seal number; and
(9) Initial meter reading.

b) Procedures must be implemented for auditing such records.

4. System software signature verification. (MICS 543.8(g)(4)

a) Procedures must be implemented for system software verifications. These procedures must include comparing signatures to the signatures provided in the independent test laboratory letter for that software version and/or the WSGC website.

b) An agent independent of operation must perform system software signature verification(s) to verify that only approved software is installed.

c) Procedures must be implemented for investigating and resolving any software verification variances.

d) Internal audits must be conducted. Such audits must be documented.

5. Installation testing. (MICS 543.8(g)(5)

a) Testing must be completed during the installation process to verify that the player interface has been properly installed. This must include testing of the following, as applicable:

(1) Communication with the gaming system;
(2) Communication with the accounting system;
(3) Communication with the player tracking system;
(4) Currency and vouchers to bill acceptor;
(5) Voucher printing;
(6) Meter incrementation;
(7) Pay table, for verification;
(8) Player interface denomination, for verification;
(9) All buttons, to ensure that all are operational and programmed appropriately;
(10) System components, to ensure that they are safely installed at location; and
(11) Locks, to ensure that they are secure and functioning.

6. Display of rules and necessary disclaimers. (MICS 543.8(g)(6)

a) The operation must ensure that all game rules and disclaimers are displayed at all times or made readily available to the player upon request,

b) TGA must verify that all game rules and disclaimers are displayed at all times or made readily available to the player upon request.

7. TGA approval of all technologic aids before they are offered for play. (MICS 543.8(g)(7)

8. All the gaming equipment must comply with 25 CFR part 547, Minimum Technical Standards for Gaming Equipment and also the Tribal-State Compact for the Class III gaming; and (MICS 543.8(g)(8)

9. In the event of a dispute by a player that cannot be resolved by ordinary means by Gaming Facility personnel as to the outcome, prize, wager

made, or any other aspect of the player's participation in a Game Set being played, all relevant data shall be immediately collected, including but not limited to all meter readings, memory records, surveillance recordings, and any other reports or information regarding play at the Terminal for the play in dispute. Following the collection of all relevant data, the TGA shall be notified and requested to make an evaluation of whether or not the dispute involves the integrity of the hardware or software being used and to try and resolve the dispute. A report of all disputes shall be maintained by the TGA. If the dispute is not resolved within 72 hours from the time of the complaint, the TGA shall immediately forward a report to the SGA detailing the nature of the dispute. In the event the dispute is resolved, the TGA is not obligated to report to the SGA but shall make TGA reports available for review. (MICS 543.8(g)(9)

B. Malfunctions. Procedures must be implemented to investigate, document and resolve malfunctions. Such procedures must address the following: (MICS 543.8(h)(1)

1. Determination of the event causing the malfunction
2. Review of relevant records, game recall, reports, logs, surveillance records;
3. Repair or replacement of the gaming component;
4. Verification of the integrity of the gaming component before restoring it to operation.

C. Removal, retirement and/or destruction. Procedures must be implemented to retire or remove any or all associated components of a gaming system from operation. Procedures must include the following (543.8(h)(2)

1. For player interfaces and components that accept cash or cash equivalents:
    a) Coordinate with the drop team to perform a final drop;
    b) Collect final accounting information such as meter readings, drop and payouts;
    c) Remove and/or secure any or all associated equipment such as locks, card reader, or ticket printer from the retired or removed component; and
    d) Document removal, retirement, and/or destruction.
2. For removal of software components:
    a) Purge and/or return the software to the license holder; and
    b) Document the removal.
3. For other related equipment such as blowers, cards, interface cards:

a) Remove and/or secure equipment; and

b) Document the removal or securing of equipment.

4. For all components:

a) Verify that unique identifiers, and descriptions of removed/retired components are recorded as part of the retirement documentation; and

b) Coordinate with the accounting department to properly retire the component in the system records.

5. Where TGA authorizes destruction of any gaming system components, procedures must be developed to destroy such components. Such procedures must include the following:

a) Methods of destruction;

b) Witness or surveillance of destruction;

c) Documentation of all components destroyed; and

d) Signatures of agent(s) destroying components attesting to destruction.

## 8.29. EGS Audit and Accounting Standards.

A. When cash is used, the following procedures shall be performed by accounting/auditing employees who are independent of the transactions being reviewed: (TSC X2 5.15)

B. For each drop period, accounting/auditing employees shall compare the report information required in Appendix X2, Section 7.1.10 (a) to the total cash acceptor drop amount for the period. Discrepancies shall be resolved before the generation/distribution of any statistical reports. (TSC X2 5.15.1)

C. TGA will be notified and follow-up shall be performed for any one machine having an unresolved variance between actual cash drop and the report information required in Appendix X2, Section 7.1.10 (a) in excess of an amount that is both more than $25 and at least three percent (3%) of the actual cash drop. The follow-up performed and results of the investigation shall be documented and maintained for inspection. (TSC X2 5.15.2)

D. At least annually, accounting/auditing and TGA personnel shall randomly verify that EPROM or other equivalent game software media changes are properly reflected in the analysis reports. (TSC X2 5.15.3)

E. Accounting/auditing employees shall review exception reports on a daily basis for propriety of transactions and unusual occurrences. TGA will be notified in writing of any unexplained or suspicious transactions or unusual occurrences. (TSC X2 5.15.4)

F. All auditing procedures and any follow-up performed shall be documented and

maintained for inspection. (TSC X2 5.15.5)

G. Cash shall be removed from the Player Terminal in accordance with Tribal-State Compact, Appendix A drop box and transportation standards for secure and verifiable handling of cash receipts from electronic games. (TSC X2 5.15.6)

# Chapter 9 COMPLIMENTARY SERVICES & ITEMS

## 9.1. Supervision

A. Supervision must be provided as required for approval of complimentary services by an agent(s) with authority greater than those being supervised. MICS 543.13(a)

## 9.2. Complimentary Services or Items

A. Controls shall be established and procedures implemented for complimentary services or items that address the following: MICS 543.13(b)

1. Agents authorized to approve the issuance of complimentary services or items, including levels of authorization, as approved by TGA;
2. Limits and conditions on the approval and issuance of complimentary services or items, as approved by TGA;
3. Making and documenting changes to conditions or limits on the approval and issuance of complimentary services or items, as approved by TGA;
4. Documenting and recording the authorization, issuance, and redemption of complimentary services or items, including cash and non-cash gifts;
    a) Records must include the following for all complimentary items and services equal to or exceeding an amount established by the gaming operation and approved by TGA:
        (1) Name of patron who received the complimentary service or item;
        (2) Name(s) of issuer(s) of the complimentary service or item;
        (3) The actual cash value of the complimentary service or item;
        (4) The type of complimentary service or item (i.e., food, beverage); and
        (5) Date the complimentary service or item was issued.

## 9.3. Complimentary Services and Items Records

A. Complimentary services and items records must be summarized and reviewed for proper authorization and compliance with established authorization thresholds. MICS 543.13(c)

1. A detailed reporting of complimentary services or items equal to or exceeding $100 or an amount established by the Tribal gaming operation, which shall not be greater than $100 must be prepared at least monthly.
2. The detailed report must be forwarded to management for review.

## 9.4. Variances

A. Any variance in excess of $25.00 shall be reviewed to determine the cause. Any such review must be documented. MICS 543.13(d)

# Chapter 10 CAGE, VAULT, KIOSK, & CASH EQUIVALENTS

## 10.1. Supervision

A. Supervision must be provided as required for cage, vault, kiosk, and other operations using cash or cash equivalents by an agent(s) with authority greater than those being supervised. MICS 543.18(a)

## 10.2. Check Cashing MICS 543.18(b)

A. If checks are cashed at the cage, the controls must provide for security and integrity. For each check cashing transaction, the agent(s) conducting the transaction must:

1. Verify the patron's identity;
2. Examine the check to ensure it includes the patron's name, current address, and signature;
3. For personal checks, verify the patron's check cashing authority and record the source and results in accordance with management policy; however
4. If a check guarantee service is used to guarantee the transaction and the procedures required by the check guarantee service are followed, then the above requirements do not apply.

B. When traveler's checks or other guaranteed drafts, such as cashier's checks, are presented, the cashier must comply with the examination and documentation procedures as required by the issuer.

C. If a third party check cashing or guarantee service is used, the examination and documentation procedures required by the service provider apply, unless otherwise provided by tribal law or regulation.

## 10.3. Cage and Vault Accountability MICS 543.18(c)

A. All transactions that flow through the cage must be summarized for each work shift of the cage and must be supported by documentation.

B. Increases and decreases to the total cage inventory must be verified, supported by documentation, and recorded. Documentation must include the date and shift, the purpose of the increase/decrease, the agent(s) completing the transaction, and the person or department receiving the cage funds (for decreases only). Unverified transfers of cash and/or cash equivalents are prohibited. (MICS 542.14(d)(2))

C. The cage and vault inventories (including coin rooms) must be counted independently by at least two agents, attested to by signature, and recorded in

ink or other permanent form at the end of each shift during which the activity took place. These agents must make individual counts to compare for accuracy and maintain individual accountability. All variances must be documented and investigated.

D. The gaming operation must establish and comply with a minimum bankroll formula to ensure the gaming operation maintains cash or cash equivalents (on hand and in the bank, if readily accessible) in an amount sufficient to satisfy obligations to the gaming operation's patrons as they are incurred. Minimum bankroll calculations shall be completed at least annually.

## 10.4. Kiosks MICS 543.18(d)

A. Kiosks must be maintained on the cage accountability and must be counted independently by at least two agents, documented, and reconciled for each increase or decrease to the kiosk inventory.

B. Currency cassettes must be counted and filled by an agent and verified independently by at least one agent, all of whom must sign each cassette.

C. Currency cassettes must be secured with a lock or tamper resistant seal and, if not placed inside a kiosk, must be stored in a secured area of the cage/vault.

D. Kiosks shall have dedicated video surveillance through the use of a fixed camera or dedicated PTZ. Coverage will be recorded in real-time, full screen, and on dedicated digital recorders. **TSC App. X2:8.4**

E. The gaming operation, subject to the approval of TGA, must develop and implement physical security controls over the kiosks. Controls should address the following: forced entry, evidence of any entry, and protection of circuit boards containing programs.

F. With regard to cashless systems, the gaming operation, subject to the approval of TGA, must develop and implement procedures to ensure that communications between the kiosk and system are secure and functioning.

G. The following reconciliation reports must be available upon demand for each day, shift, and drop cycle (this is not required if the system does not track the information, but system limitation(s) must be noted):

1. Starting balance dollar amount per financial instrument;
2. Starting balance number of items per financial instrument;
3. Dollar amount per financial instrument issued;
4. Number of items per financial instrument issued;
5. Dollar amount per financial instrument issued;
6. Number of items per financial instrument redeemed;

7. Dollar amount per financial instrument increases;
8. Number of items per financial instrument increases;
9. Dollar amount per financial instrument decreases;
10. Number of items per financial instrument decreases;
11. Ending balance dollar amount per financial instrument; and
12. Ending balance number of items per financial instrument.

## 10.5. Patron Deposited Funds MICS 543.18(e)

A. If a gaming operation permits a patron to deposit funds with the gaming operation at the cage, and when transfers of patron deposited funds are transferred to a gaming area for wagering purposes, the following standards apply:

1. The receipt or withdrawal of a patron deposit must be documented, with a copy given to the patron and a copy remaining in the cage.
2. Both copies of the document of receipt or withdrawal must contain the following information:
    a) Same receipt number on each copy;
    b) Patron's name and signature;
    c) Date of receipt and withdrawal;
    d) Dollar amount of deposit/withdrawal (for foreign currency transactions include the US dollar equivalent, the name of the foreign country, and the amount of the foreign currency by denomination);
    e) Nature of deposit/withdrawal; and
    f) Name and signature of the agent who conducted the transaction.
3. Procedures must be established and complied with for front money deposits to:
    a) Maintain a detailed record by patron name and date of all funds on deposit;
    b) Maintain a current balance of all patron deposits that are in the cage/vault inventory or accountability; and
    c) Reconcile the current balance with the deposits and withdrawals at least daily.

## 10.6. Promotional Payments, Drawings, and Giveaway Programs MICS 543.18(f)

A. The following procedures must apply to any payment resulting from a promotional payment, drawing, or giveaway program disbursed by the cage department or any other department. This section does not apply to payouts for card game promotional pots and/or pools.

B. All payments must be documented to support the cage accountability.

C. Payments above $500 must be documented at the time of the payment, and documentation must include the following:

1. Date and time;
2. Dollar amount of payment or description of personal property;
3. Reason for payment; and
4. Patron's name and confirmation that identity was verified (drawings only).
5. Signature(s) of at least two agents verifying, authorizing, and completing the promotional payment with the patron. For computerized systems that validate and print the dollar amount of the payment on a computer generated form, only one signature is required.

## 10.7. Chip(s) MICS 543.18(g)

A. Controls must be established and procedures implemented to ensure accountability of chip inventory. Such controls must include, but are not limited to, the following:

1. Purchase;
2. Receipt;
3. Inventory;
4. Storage; and
5. Destruction.

## 10.8. Vouchers MICS 543.18(h)

A. Controls must be established and procedures implemented to:

1. Verify the authenticity of each voucher redeemed.
2. If the voucher is valid, verify that the patron is paid the appropriate amount.
3. Document the payment of a claim on a voucher that is not physically available or a voucher that cannot be validated such as a mutilated, expired, lost, or stolen voucher.
4. Retain payment documentation for reconciliation purposes.

5. For manual payment of a voucher of $500 or more, require a supervisory employee to verify the validity of the voucher prior to payment.

B. Vouchers paid during a period while the voucher system is temporarily out of operation must be marked “paid” by the cashier.

C. Vouchers redeemed while the voucher system was temporarily out of operation must be validated as expeditiously as possible upon restored operation of the voucher system.

D. Paid vouchers must be maintained in the cashier's accountability for reconciliation purposes.

E. Unredeemed vouchers can only be voided in the voucher system by supervisory employees. The accounting department will maintain the voided voucher, if available.

## 10.9. Cage and Vault Access

A. Controls must be established and procedures implemented to: **MICS 543.18(i)**

1. Restrict physical access to the cage to cage agents, designated staff, and other authorized persons; and
2. Limit transportation of extraneous items such as personal belongings, tool boxes, beverage containers, etc., into and out of the cage.
3. As part of the Gaming Operation there shall be on or immediately adjacent to the gaming floor a physical structure known as the Cashier's Cage to house the cashiers and to serve as the central location for the following **(TSC App A:7(1))**:
    a) The custody of the cage inventory comprising currency, coin, patron checks, gaming chips, forms, documents and records normally associated with the operation of a cage.
    b) The approval of patron checks for the purpose of gaming in conformity with these standards
    c) The receipt, distribution, and redemption of gaming chips in conformity with these standards
4. Cashiers functions will be, but are not limited to the following **(TSC App A:8(2))**:
    a) Receive currency, coin, checks, gaming chips, vouchers, or Cash Equivalents from patrons for gaming chip consolidations, total or partial redemptions or substitutions
    b) Receive documentation with signatures thereon, required to be prepared for the effective segregation of functions in the cashier's cage

c) Process fills and Credits by exchanging chips, currency, coin and paperwork as authorized in these standards

d) Receive currency and coin from count rooms and kiosks

e) Prepare the overall cage reconciliation and accounting records

f) Perform such other functions as necessary to ensure proper accountability consistent with these standards

g) Such other functions normally associated with the operation of a cage.

5. Each cage will be designed and constructed to provide maximum security including, at a minimum, the following **(TSC App A:7(4)):**

a) An enclosed structure except for openings through which items such as gaming chips, checks, cash, records, and documents can be passed to service the public and gaming stations

b) Manually triggered silent alarm systems connected directly to the monitoring rooms of the Surveillance System

c) Access will be through a locked door

d) The system shall have Surveillance System coverage which will be monitored by the surveillance department

6. The Tribal Gaming Operation will place on file with the Tribal Gaming Agency the names of all persons authorized to enter the cage, those who possess the combination or the Keys or who control the mechanism to open the locks securing the entrance to the cage, and those who possess the ability to operate the alarm system. **TSC App. A:7(5)**

## 10.10. Collection/Recording Checks Returned after Deposit **TSC App. A:13**

A. All dishonored checks returned by a bank ("returned checks") after deposit shall be returned directly to, and controlled by accounting department employees.

B. No person other than one employed within the accounting department may engage in efforts to collect returned checks except that a collection company or an attorney-at-law representing the tribal gaming operation may bring action for such collection. Any verbal or written communication with patrons regarding collection efforts, shall be documented in the collection section.

C. Continuous records of all returned checks shall be maintained by accounting department employees. Such records shall include, at a minimum, the following:

1. The date of the check;

2. The name and address of the drawer of the check;

3. The amount of the check;

4. The date(s) the check was dishonored;

5. The date(s) and amount(s) of any collections received on the check after being returned by a bank.
6. The date and any amount written-off as uncollectible.

D. A check dishonored by a bank may be immediately re-deposited if there is sufficient reason to believe the check will be honored the second time.

E. If a check is dishonored a second time, the name of the person who submitted the check shall be kept in a log, and available to the cashier. Such person shall be prohibited from submitting a future check until the amount owed is paid in full.

F. Any checks processed through an outside check guarantee company will not be subject to the provisions of (A) through (E) above unless the Tribal Gaming Operation chooses not to use their guarantee service to pre-approve a particular check.

## 10.11. Variances

A. The operation must establish, as approved by TGA, the threshold level at which a variance must be reviewed to determine the cause. This threshold must not exceed $50.00. Any such review must be documented. MICS 543.18(j)

# Chapter 11 INFORMATION TECHNOLOGY & DATA

A system is any computerized system that is integral to the gaming environment. This includes, but is not limited to, the server and peripherals for the gaming systems, accounting, surveillance, essential phone system, and door access and warning systems. 543.20(b)

## 11.1. Supervision 543.20(a)

A. Controls must identify the supervisory agent in the department or area responsible for ensuring that the department or area is operating in accordance with established policies and procedures.

B. The supervisory agent must be independent of the operation of the EGM.

C. Controls must ensure that duties are adequately segregated and monitored to detect procedural errors and to prevent the concealment of fraud.

D. Information technology agents having access to the gaming systems may not have signatory authority over financial instruments and payout forms and must be independent of and restricted from access to:

1. Financial instruments;
2. Accounting, audit, and ledger entries; and
3. Payout forms.

## 11.2. Controls

A. Controls must be established and procedures implemented to ensure adequate: MICS 543.20(c)

1. Control of physical and logical access to the information technology environment, including accounting, voucher, cashless and player tracking systems, among others used in conjunction with electronic gaming;
2. Physical and logical protection of storage media and its contents, including recovery procedures;
3. Access credential control methods;
4. Record keeping and audit processes; and
5. Departmental independence, including, but not limited to, means to restrict agents that have access to information technology from having access to financial instruments.

## 11.3. Physical Security 543.20(d)

A. The information technology environment and infrastructure must be maintained in a secured physical location such that access is restricted to authorized agents only.

B. Access devices to the systems' secured physical location, such as keys, cards, or fobs, must be controlled by an independent agent.

C. Access to the systems' secured physical location must be restricted to agents in accordance with established policies and procedures, which must include maintaining and updating a record of agents granted access privileges.

D. Network Communication Equipment must be physically secured from unauthorized access.

## 11.4. Logical Security 543.20(e)

A. Controls must be established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured:

1. Systems' software and application programs;
2. Data associated with electronic gaming; and
3. Communications facilities, systems, and information transmissions associated with the gaming systems.

B. Unused services and non-essential ports must be disabled whenever possible.

C. Procedures must be implemented to ensure that all activity performed on systems is restricted and secured from unauthorized access, and logged.

D. Communications to and from systems via Network Communication Equipment must be logically secured from unauthorized access.

## 11.5. User Controls 543.20(f)

A. Systems, including application software, must be secured with passwords or other means for authorizing access.

B. Management personnel or agents independent of the department being controlled must assign and control access to system functions.

C. Access credentials such as passwords, PINs, or cards must be controlled as follows:

1. Each user must have his or her own individual access credential;
2. Access credentials must be changed at an established interval approved by TGA; and
3. Access credential records must be maintained either manually or by systems that automatically record access changes and force access credential changes, including the following information for each user:

a) User's name;

b) Date the user was given access and/or password change; and

c) Description of the access rights assigned to user.

D. Lost or compromised access credentials must be deactivated, secured or destroyed within an established time period approved by TGA.

E. Access credentials of terminated users must be deactivated within an established time period approved by the TGA.

F. Only authorized agents may have access to inactive or closed accounts of other users, such as player tracking accounts and terminated user accounts.

## 11.6. Personnel Access Listing Standards TSC App. A:7(5); X2:9.7

A. A personnel access listing for the Player Account Server and all computerized gaming systems shall be maintained which includes at a minimum:

1. Employee name;
2. Employee identification number (or equivalent); and
3. Listing of functions each employee can perform or equivalent means of identifying this information.

## 11.7. Installations and/or Modifications 543.20(g)

A. Only TGA authorized or approved systems and modifications may be installed.

B. Records must be kept of all new installations and/or modifications to the gaming systems. These records must include, at a minimum:

1. The date of the installation or modification;
2. The nature of the installation or change such as new software, server repair, significant configuration modifications;
3. Evidence of verification that the installation or the modifications are approved; and
4. The identity of the agent(s) performing the installation/modification.

C. Documentation must be maintained, such as manuals and user guides, describing the systems in use and the operation, including hardware.

## 11.8. Remote Access 543.20(h)

A. Except for Tribal Lottery and Surveillance systems, Agents may be granted remote access for system support, provided that each access session is documented and maintained at the place of authorization. The documentation must include:

1. Name of agent authorizing the access;

2. Name of agent accessing the system;
3. Verification of the agent's authorization;
4. Reason for remote access;
5. Description of work to be performed;
6. Date and time of start of end-user remote access session; and
7. Date and time of conclusion of end-user remote access session.

B. If authorized by Tribal-State Compact (TSC) Memorandums of Understanding (MOU), remote access for the Tribal Lottery Systems and Surveillance System will be permitted according to the precise conditions of the agreement. Remote access to these systems is not permitted until TSC MOU's for this purpose are agreed to, and TGA has approved procedures developed by TGO to meet the conditions of each agreement.

C. All remote access must be performed via a secured method as authorized by CTGC.

D. Remote access to the Tribal Lottery System shall only be authorized in accordance with an approved MOU between the Cowlitz Tribe and the State of Washington.

## 11.9. Incident Monitoring and Reporting 543.20(i)

A. Procedures must be implemented for responding to, monitoring, investigating, resolving, documenting, and reporting security incidents associated with information technology systems.

B. All security incidents must be responded to within 72 hours and formally documented with in fourteen (14) days .

C. A report shall be created within 30 days of the security incident. Such report(s) shall be distributed to the IT Director, Compliance Officer and CTGC. The Compliance Department shall report any items required by Title 31 to FinCEN.

## 11.10. Data Backups 543.20(j)

A. Controls, as approved by TGA must include adequate backup, including, but not limited to, the following:

1. Daily data backup of critical information technology systems;
2. Data backup of critical programs or the ability to reinstall the exact programs as needed;
3. Secured storage of all backup data files and programs, or other adequate protection;
4. Mirrored or redundant data source; and
5. Redundant and/or backup hardware.

B. Controls, as approved by TGA must include recovery procedures, including, but not limited to, the following:

1. Data backup restoration;
2. Program restoration; and
3. Redundant or backup hardware restoration.

C. Recovery procedures must be tested on a sample basis at specified intervals at least annually. Results must be documented.

D. Backup data files and recovery components must be managed with at least the same level of security and access controls as the system for which they are designed to support.

## 11.11. Software Downloads 543.20(k)

A. Downloads, either automatic or manual, must be performed in accordance with 25 CFR 547.12.

## 11.12. Verifying Downloads 543.20(l)

A. Following download of any gaming system software, the gaming system must verify the downloaded software using a software signature verification method. Using any method it deems appropriate, TGA must confirm the verification.

# Chapter 12 SURVEILLANCE

## 12.1. Supervision

A. Supervision must be provided as required for surveillance by an agent(s) with authority greater than those being supervised. **MICS 543.21(a)**

## 12.2. Surveillance Equipment and Control Room(s) **MICS 543.21(b)**

A. Controls must be established and procedures implemented that include the following:

1. The surveillance system must be maintained and operated from a staffed surveillance operation room(s).
2. The surveillance operation room(s) must be secured to prevent unauthorized entry.
3. Entrances to the Surveillance System monitoring room(s) shall not be visible from the Gaming Facility area.
4. Access to the surveillance operation room(s) must be limited to surveillance agents, agents of the Tribal Gaming Agency, State Gaming Agency, and those specifically authorized by TGA.
5. Surveillance operation room(s) access logs must be maintained.
6. Surveillance operation room equipment must have total override capability over all other satellite surveillance equipment.
7. Power loss to the surveillance system:
    a) In the event of power loss to the surveillance system, an auxiliary or backup power source must be available and capable of providing immediate restoration of power to the surveillance system to ensure that surveillance agents can observe all areas covered by dedicated cameras.
8. The surveillance system must record an accurate date and time stamp on recorded events. The displayed date and time must not significantly obstruct the recorded view.
9. All surveillance agents must be trained in the use of the equipment, games, and house rules.
10. Each camera required by the standards in this section must be installed in a manner that will prevent it from being readily obstructed, tampered with, or disabled.
11. A periodic inspection of the surveillance systems must be conducted. When a malfunction of the surveillance system is discovered, the malfunction and necessary repairs must be documented, and repairs initiated within seventy- two (72) hours. **MICS 543.21(b)(11)**

a) If a dedicated camera malfunctions, alternative security procedures, such as additional supervisory or security agents, must be implemented immediately; and **MICS 543.21(b)(11)(i)**

b) TGA must be notified of any surveillance system and/or camera(s) that have malfunctioned for more than twenty-four (24) hours and the alternative security measures being implemented. **MICS 543.21(b)(11)(ii)**

12. The surveillance system must:

a) Have the capability to display all camera views on a monitor;

b) Include sufficient numbers of recording devices to record the views of all cameras required by this section;

c) Record all camera views required by this section;

d) Include sufficient numbers of monitors to simultaneously display gaming and count room activities;

e) Have light sensitive cameras with zoom, scan and tilt capabilities to effectively and clandestinely monitor in detail and from various vantage point the following: App A:21(2)(a)

(1) The Gaming activities conducted in the Gaming Facility;

(2) ii. The operations conducted at the cashier's cage and keno cage;

(3) The entire count process and any other activities conducted in the count room and the storage cabinets or trolleys used to store Drop Boxes;

(4) The movement of cash, gaming chips, and Drop Boxes in the establishment; and

(5) The entrances and exits to the Gaming Facility and the count rooms.

(6) Such other areas as the Tribal Gaming Agency designates.

f) Digital images record and playback images with sufficient magnification and clarity that shows fluid motion and allows the viewer to clearly distinguish the value of currency, coins, gaming chips, playing cards, and outcome of the game and effectively monitor in detail all areas in the gaming facility where Class III gaming is conducted, including but not limited to table games; TLS; poker; keno stations; cages; count rooms; information technology department; and all gaming activity conducted by gaming employees, patrons or players; AAR-2017-01

g) Be capable of audio recording the entire count process and any other activities in the count room; TSC App. A:2(d)

h) Be equipped with an alarm that notifies the operator in the event of an equipment malfunction.

i) Be password protected with only system administrator user rights having the password to disable the erase and reformat functions.

13. Adequate lighting shall be present in all areas, including the gaming floor, where Surveillance System coverage is required.

14. Digital surveillance suppliers may have periodic access to perform routing upgrades and maintenance under the following conditions:

a) TGA must approve the remote access prior to it occurring;

b) A log must be kept of the remote access to include who is accessing, time length of the remote access connection, and the address of the remote connection.

c) All supplier representatives remotely accessing the Surveillance System must be licensed by the Tribe and Certified by the State Gaming Agency.

d) At no time will the supplier representatives have access to manipulate or change live or recorded camera coverage.

## 12.3. Progressive Prize Meters Surveillance Standards

A. Surveillance of the progressive prize meters for the gaming systems at the following thresholds:

1. Wide area progressives for Class II gaming with a reset amount of $1 million; and

2. In-house progressives with a reset amount of $250,000.

B. Except as otherwise provided in paragraph (A)(1) of this section, gaming machines offering a payout of more than $250,000 shall be monitored and recorded by a dedicated camera(s) to provide coverage of:

1. All customers and employees at the gaming machine, and

2. The face of the gaming machine, with sufficient clarity to identify the payout line(s) of the gaming machine.

C. Progressive table games with a progressive jackpot of $25,000 or more shall be monitored and recorded by dedicated cameras that provide coverage of:

1. The table surface, sufficient that the card values and card suits can be clearly identified;

2. An overall view of the entire table with sufficient clarity to identify customers and dealer; and

3. A view of the progressive meter jackpot amount. If several tables are linked to the same progressive jackpot meter, only one meter need be recorded.

## 12.4. Other Compact Minimum Requirement

A. Minimum surveillance coverage including, but not limited to the following: TSC App. A:6(3)(vi)

1. The detection of cheating, theft, embezzlement, and other illegal activities in the gaming facility, count rooms, and cashier's cage;
2. The video taping of illegal and unusual activities monitored;
3. The notification of appropriate gaming facility supervisors, and TGA upon the detection and taping of cheating, theft, embezzlement, or other illegal activities;

B. No present or former surveillance department employee shall be employed in any other capacity in the tribal gaming operation unless the Tribal Gaming Agency, upon petition approves such employment in a particular capacity upon a finding that: TSC App. A:6(3)(vii)

1. One year has passed since the former surveillance department employee worked in the surveillance department; and
2. Surveillance and security systems will not be jeopardized or compromised by the proposed employment of the former surveillance department employee in the capacity proposed; and
3. Errors, irregularities, or illegal acts cannot be perpetrated and concealed by the former surveillance department employee's knowledge of the surveillance system in the capacity in which the former surveillance department employee will be employed.

## 12.5. Card Games/Table Games Surveillance Standards MICS 543.21(c)(3)

A. Except for tournaments, a dedicated camera(s) with sufficient clarity must be used to provide:

1. An overview of the activities on each table surface, including card faces and cash and/or cash equivalents;
2. An overview of table/card game activities, including patrons and dealers; and
3. An unobstructed view of all posted progressive pool amounts

B. For tournaments, a dedicated camera(s) must be used to provide an overview of tournament activities, and any area where cash or cash equivalents are exchanged.

## 12.6. Cage and Vault Surveillance Standards MICS 543.21(c)(4)

A. The surveillance system must monitor and record a general overview of activities occurring in each cage and vault area with sufficient clarity to identify individuals within the cage and patrons and staff members at the counter areas and to confirm the amount of each cash transaction;

B. Each cashier station must be equipped with one (1) dedicated overhead camera covering the transaction area; and

C. The cage or vault area in which exchange and transfer transactions occur must be monitored and recorded by a dedicated camera or motion activated dedicated camera that provides coverage with sufficient clarity to identify the chip values and the amounts on the exchange and transfer documentation. Controls provided by a computerized exchange and transfer system constitute an adequate alternative to viewing the amounts on the exchange and transfer documentation.

## 12.7. Kiosk TSC App.X2:8.4; MICS 543.21(c)(6)

A. The surveillance system must monitor and record a general overview of activities occurring at each kiosk with sufficient clarity to identify the activity and the individuals performing it, including maintenance, drops or fills, and redemption of wagering vouchers or credits.

## 12.8. Count Rooms Surveillance Standards MICS 543.21(c)(5); TSC App. A:6(3)(b)(iii)

A. The surveillance system must monitor and record with sufficient clarity a general overview of all areas where cash or cash equivalents may be stored or counted; and

B. The surveillance system must provide coverage of count equipment with sufficient clarity to view any attempted manipulation of the recorded data; and

C. Audio capability in the count rooms.

## 12.9. Reporting Requirements MICS 543.21(d)

A. TGA-approved procedures must be implemented for reporting suspected crimes and suspicious activity.

## 12.10. Recording Retention MICS 543.21(e)

A. Controls must be established and procedures implemented that include the following:

1. All recordings required by this section must be retained for a minimum of seven (7) days; and

2. Upon request of TGA or the State Gaming Agency, thirty (30) days, or for

such longer period as may be required.

3. Suspected crimes, suspicious activity, or detentions by security agents discovered within the initial retention period must be copied and retained for a time period, not less than 1 year.

## 12.11. Logs MICS 543.21(f)

A. Logs must be maintained and demonstrate the following:

1. Compliance with the storage, identification, and retention standards required in this section;
2. Each malfunction and repair of the surveillance system as defined in this section; and
3. Activities performed by surveillance agents as required by the controls in this section.

B. The surveillance logs shall include, at a minimum, the following:

1. Date and time of surveillance;
2. Person initiating surveillance;
3. Reason for surveillance;
4. Time of termination of surveillance;
5. Summary of the results of the surveillance;
6. A record of any equipment or camera malfunctions

# Chapter 13 Drop & Count Minimum Internal Control Standards

## 13.1. Supervision MICS 543.17(a)

A. Supervision must be provided for drop and count as needed by an agent(s) with authority greater than those being supervised.

## 13.2. Drop Boxes, Transportation to and from Gaming Station and Storage in the Count Room TSC App. A:10

A. All Drop Boxes removed from the gaming stations, player terminals, or kiosks will be transported, at a minimum, by one Security Department Member and one employee of the Tribal Gaming Operation directly to, and secured in, the count room.

B. All Drop Boxes, not attached to a gaming station, will be stored in the count room in an enclosed storage cabinet or trolley and secured in such cabinet or trolley by a separately keyed, double locking system. The Key to one lock will be maintained and controlled by the security department and the Key to the second lock will be maintained and controlled by the Tribal Gaming Agency Inspector.

1. Alternatively, empty emergency drop cans may be stored in accordance to 6-AAR-2017-04 provided the gaming operation establishes a system of internal controls as approved by the Tribal Gaming Agency.

C. Drop Boxes, when not in use during a shift may be stored on the gaming stations provided that there is adequate security. If adequate security is not provided during this time, the Drop Boxes will be stored in the count room in an enclosed storage cabinet or trolley as required in paragraph B.

## 13.3. Count Room Characteristics TSC App. A:18

A. As part of the gaming operation, there shall be a room specifically designated for counting the contents of drop boxes which shall be known as the count room.

B. The count room shall be designed and constructed to provide maximum security for the materials housed therein and for the activities conducted therein, to include at a minimum, the following:

1. A door equipped with two separate locks securing the interior of the count room. The keys to which shall be different from any other Keys. One key shall be maintained, controlled and accessible by the security department in a secure area, and the other key maintained and controlled by a different gaming department or TGA;
2. The security department shall establish a sign out procedure for all keys removed from the security department; and

3. An alarm device connected to the entrance of the count room in such a manner as to cause a signal to the monitors of the surveillance system whenever the door to the count room is opened.

C. Located within the count room shall be:

1. A table constructed of clear glass or similar material for the emptying, counting and recording of the contents of the drop boxes which shall be known as the "Count Table";

2. Surveillance cameras and microphones wired to monitoring rooms capable of, but not limited to the following: **TSC App. A:21(2)(iii)**

a) Effective, detailed video and audio monitoring and recording of the entire count process and any other activities in the count room;

b) Effective, detailed video-monitoring of the count room, including storage cabinets or trolleys used to store drop boxes.

## 13.4. Count Room Access MICS 543.17(b)

A. Controls must be established and procedures implemented to limit physical access to the count room to count team agents, designated staff, and other authorized persons. Such controls must include the following:

1. The Count room access list shall be submitted to TGA for approval.

a) The approved Count room access list shall be posted in clear view near the entrance of the Count room.

2. Count team agents may not exit or enter the count room during the count except for emergencies or scheduled breaks. All count room team agents shall observe the same scheduled breaks.

3. TGA may elect to have an Inspector present during the count.

4. Surveillance must be notified immediately prior to the commencement of the count and whenever count room agents exit or enter the count room during the count.

5. The count team policy, at a minimum, must address the transportation of extraneous items such as personal belongings, toolboxes, beverage containers, etc., into or out of the count room.

## 13.5. Count Team MICS 542.41(c)

A. Controls must be established and procedures implemented to ensure security of the count and the count room to prevent unauthorized access, misappropriation of funds, forgery, theft, or fraud. Such controls must include the following:

1. All counts must be performed by at least three agents.

2. At no time during the count can there be fewer than three count team agents in the count room until the drop proceeds have been accepted into cage/vault accountability.
3. Count team agents must be rotated on a routine basis such that the count team is not consistently the same three agents more than four days per week. This standard does not apply to gaming operations that utilize a count team of more than three agents.
4. Functions performed by count team agents must be rotated on a routine basis.
5. Count team agents must be independent of the department being counted. A cage/vault agent may be used if they are not the sole recorder of the count and do not participate in the transfer of drop proceeds to the cage/vault. An accounting agent may be used if there is an independent audit of all count documentation.

## 13.6. Card & Table Games Drop Standards MICS 543.17(d)

A. Controls must be established and procedures implemented to ensure security of the drop process. Such controls must include the following:

1. Surveillance must be notified when the drop is to begin so that surveillance may monitor the activities.
2. At least two agents must be involved in the removal of the drop box, at least one of whom is independent of the card/table games department. At least one of whom is a member of the Security Department (TSC App. A:10(1)).
3. Once the drop is started, it must continue until finished.
4. All drop boxes may be removed only at the time previously designated by the gaming operation and reported to the TGA. If an emergency drop is required, surveillance must be notified before the drop is conducted and the TGA must be present for transport in accordance with 6-AAR-2017-05.
5. At the end of each shift:
    a) All locked card/table game drop boxes must be removed from the tables by an agent independent of the card/table game shift being dropped;
    b) For any tables opened during the shift, a separate drop box must be placed on each table, or a gaming operation may utilize a single drop box with separate openings and compartments for each shift; and
    c) Card/Table game drop boxes must be transported directly to the count room by a minimum of two agents, at least one of whom is

independent of the card/table game shift being dropped, until the count takes place and at least one of whom is a member of the Security Department (TSC App. A:10(1)).

6. All tables that were not open during a shift and therefore not part of the drop must be documented.
7. All card/table game drop boxes must be posted with a number corresponding to a permanent number on the gaming table and marked to indicate game, table number, and shift, except that emergency drop boxes may be maintained without such number or marking, provided the word "emergency" is permanently imprinted or impressed thereon and, when put into use, are temporarily marked with the number of the gaming station and identification of the game and shift.
8. One separate lock securing the contents placed into the drop box, the key to which shall be different from any other key (TSC App. A:9(2)(a)).
9. A separate lock securing the drop box to the gaming stations, the key to which shall be different from the key to the lock securing the contents of the drop box (TSC App. A:9(2)(b).
10. The key utilized to unlock the drop boxes from the gaming stations shall be maintained and controlled by the security department (TSC App. A:9(3)).
11. The key to the lock securing the contents of the drop boxes shall be maintained and controlled by TGA (TSC App. A:9(4)).

## 13.7. EGM Drop Standards MICS 542.41(e)

A. Surveillance must be notified when the drop is to begin so that surveillance may monitor the activities.

B. At least two agents must be involved in the removal of EGM drop boxes, at least one of whom is independent of the player interface department.

C. All drop boxes may be removed only at the time previously designated by the gaming operation and reported to the TGA. If an emergency drop is required, surveillance must be notified before the drop is conducted and the TGA present for transport in accordance with **6-AAR-2017-05**.

D. The drop boxes must be removed by an agent independent of the Slot Department, then transported directly to the count room or other equivalently secure area with comparable controls and locked in a secure manner until the count takes place.

1. Security must be provided for the drop boxes removed from player terminals and awaiting transport to the count room.
2. Transportation of drop boxes must be performed by a minimum of two agents, at least one of whom is independent of the Slot Department and one of whom must be a member of the Security Department.

E. All drop boxes must be posted with a number corresponding to a permanent number on the player terminal.

1. In the event “smart cans” are used, the gaming station number will be maintained on a chip located in each individual drop can. The chip will track the gaming station, player terminal or kiosk number and may be cleared and reset as approved by the Tribal Gaming Agency. (TSC App. A:9(2)(d)(iii))

## 13.8. Count Standards MICS 543.17(g)

A. Access to stored, full drop boxes must be restricted to:

1. Authorized members of the drop and count teams; and
2. In an emergency, authorized persons for the resolution of a problem.

B. The count must be performed in the count room.

C. The TGO will, at a minimum count the contents of Drop Boxes once each gaming day.

D. Access to the count room during the count must be restricted to members of the drop and count teams, with the exception of authorized Inspectors, supervisors for resolution of problems, and authorized maintenance personnel.

E. If counts from various revenue centers occur simultaneously in the count room, procedures must be in effect to prevent the commingling of funds from different revenue centers.

F. Count equipment and systems must be tested, with the results documented, at minimum before the first count begins to ensure the accuracy of the equipment.

G. The drop boxes must be individually emptied and counted so as to prevent the commingling of funds between boxes until the count of the box has been recorded.

1. The count of each box must be recorded in ink or other permanent form of recordation.
2. Coupons or other promotional items not included in gross revenue must be recorded on a supplemental document by either the count team members or accounting personnel. All single-use coupons must be cancelled daily by an authorized agent to prevent improper recirculation.
3. If a currency counter interface is used:

a) It must be restricted to prevent unauthorized access; and

b) The currency drop figures must be transferred via direct communications line or computer storage media to the accounting department.

H. Procedures and requirements for conducting the count shall be the following: TSC App. A:19(6)

1. As each Drop Box is placed on a count table, one count team member shall announce, in a tone of voice to be recorded by the audio recording device, the game, station number, and shift marked thereon or as displayed by the barcode scanner or "smart can" reader;
2. The contents of each Drop Box shall be emptied and counted separately, and at all times be conducted in full view of the Surveillance System cameras located in the count room;
3. Immediately after the contents of a Drop Box are emptied, the inside of the Drop Box shall be held up to the full view of a Surveillance System camera, and shall be shown to at least one other count team member to confirm that all contents of the Drop Box have been removed, after which the Drop Box shall be locked and placed in the storage area for Drop Boxes;
4. The contents of each Drop Box shall be segregated by a count team member or currency counter into separate stacks by coin and currency and by type of form, record or document;
5. Each denomination of coin and currency shall be counted twice by the count team members manually or using currency counters in full view of the Surveillance System cameras, and such count shall be observed and the accuracy confirmed orally or in writing, by at least two separate count team members. When using a currency counter and the two counts do not agree, the monies will be pulled and be re-processed. If the counts from the second attempt do not agree or the currency counter malfunctions, the currency will be counted manually;
6. As the contents of each Drop Box is counted for gaming stations, one count team member shall record or verify on a Master Game Report, by game, station number, and shift, the following information:
    a) The total amount of currency and coin counted;
    b) The amount of the Opener;
    c) The amount of the Closer;
    d) The serial number and amount of each Fill;
    e) The total amount of all Fills;
    f) The serial number and amount of each Credit;
    g) The total amount of all Credits; and
    h) The win or loss
    i) Such additional information as may be required on the Master Game Report by TGO

7. As the contents of each Drop Box are counted for a player terminal or kiosk, one count team member shall record the box number and the total amount of currency counted. The Tribal Lottery System counts will be compared to the system reports. The count team must not have access to amount-in or bill-in meter amounts until after the count is completed and the drop proceeds are accepted into the cage/vault accountability.

8. Notwithstanding the requirements of sub-paragraphs 6 and 7, if the Tribal Gaming Operation's system of accounting and internal controls provides for the recording on the Master Game Report of fills, Credits, and station inventory slips by Cage Cashiers prior to the commencement of the count, a count team member shall compare for agreement the serial numbers and totals of the amounts recorded thereon to the fills, Credits, and station inventory slips removed from the Drop Boxes;

9. Notwithstanding the requirements of sub-paragraphs 6 and 7, if the Tribal Gaming Operation's system of accounting and internal controls provides for the count team functions to be comprised only of counting and recording currency, coin, and Credits; Accounting Department employees shall perform all other counting, recording and comparing duties herein;

10. After completion and verification of the Master Game Report, each count team member shall sign the report attesting to the accuracy of the information recorded thereon;

11. At no time after the Inspector has signed the Master Game Report shall any change be made to it without prior written approval of the Tribal Gaming Agency.

12. Procedures must be implemented to ensure that any corrections to the count documentation are permanent, identifiable and the original, corrected information remains legible. Corrections must be verified by two count team agents. **MICS 543.17(g)(12)**

13. The count sheet must be reconciled to the total drop by a count team member who may not function as the sole recorder, and variances must be reconciled and documented. This standard does not apply to vouchers removed from the financial instrument storage components. **MICS 543.17(g)(13)**

I. If currency counters are utilized, a count team member must observe the loading and unloading of all currency at the currency counter, including rejected currency. **MICS 543.17(g)(9)**

J. Two counts of the currency rejected by the currency counter must be recorded per interface terminal as well as in total. Rejected currency must be posted to the player interface from which it was collected. **MICS 543.17(g)(10)**

K. A final verification of the total drop proceeds, before transfer to cage/vault must be performed by at least two agents, one of whom is a supervisory count team member, and one a count team agent. **MICS 543.17(g)(15)(i-v)**

1. Final verification must include a comparison of currency counted totals against the currency counter/system report, if any counter/system is used.
2. Any unresolved variances must be documented, and the documentation must remain part of the final count record forwarded to accounting.
3. This verification does not require a complete recount of the drop proceeds but does require a review sufficient to verify the total drop proceeds being transferred.
4. The two agents must sign the report attesting to the accuracy of the total drop proceeds verified.
5. All drop proceeds and cash equivalents that were counted must be turned over to the cage or vault cashier (who must be independent of the count team) or to an agent independent of the revenue generation and the count process for verification. Such cashier or agent must certify, by signature, the amount of the drop proceeds delivered and received. Any unresolved variances must be reconciled, documented, and/or investigated by accounting/revenue audit.
6. Procedures and requirements at the conclusion of the count shall be the following: **TSC App. A:7**
    a) All cash removed from each Drop Box after the initial count shall be presented in the count room by a count team member to a cashier who, prior to having access to the information recorded on the Master Game Report and in the presence of the count team and the Inspector, shall re-count, either manually or mechanically, the cash received, after which the Inspector shall sign the report evidencing his or her presence during the count and the fact that both the cashier and count team have agreed on the total amount of cash counted;
    b) The top copy of the Master Game Report, after signing, and the requests for fills, the fills, the requests for Credits, the Credits, and the station inventory slips removed from Drop Boxes shall be

transported directly to the Accounting Department and shall not be available to any cashier's cage personnel;

c) A duplicate of the Master Game Report, but no other document referred to in this standard whatsoever, shall be retained by the Inspector.

d) If the Tribal Gaming Operation's system of accounting and internal controls does not provide for the forwarding from the cashier's cage of the duplicate of the fills, Credits, Request for Credits, Request for Fills, such documents recorded or to be recorded on the Master Game Report shall be transported from the count room directly to the Accounting Department.

e) Only required personnel shall be present in the count room during the buy process (ie; count team, cage cashier, CTGC).

L. After certification by the agent receiving the funds, the drop proceeds must be transferred to the cage/vault. **MICS 543.17(g)(16)(i, iii, iv)**

1. The count documentation and records must not be transferred to the cage/vault with the drop proceeds.
2. All count records must be forwarded to accounting secured and accessible only by accounting agents.
3. The cage/vault agent receiving the transferred drop proceeds must sign the count sheet attesting to the verification of the total received, and thereby assuming accountability of the drop proceeds, and ending the count.

M. The originals and copies of the Master Game Report, Request for Fills, Fills, Request for Credits, Credits and station inventory slips shall on a daily basis, in the Accounting Department be: **TSC App. A:8**

1. Compared for agreement with each other, on a test basis, by persons with no recording responsibilities and, if applicable, to triplicates or stored data;
2. Reviewed for the appropriate number and propriety of signatures on a test basis;
3. Accounted for by series numbers, if applicable;
4. Tested for proper calculation, summarization, and recording;
5. Subsequently recorded; and
6. Maintained and controlled by the Accounting Department.

## 13.9. Kiosk

A. Collecting currency cassettes and financial instrument storage components from kiosk. Controls must be established and procedures implemented to ensure that currency cassettes and financial instrument storage components are securely removed from kiosks. These controls shall include Controlled Keys as outlined in 13.10 below. Such controls must include the following: **MICS 543.17(h)**

1. Surveillance must be notified prior to and monitor the cash boxes, coin hoppers, and/or currency cassettes being accessed in a kiosk.
2. At least two agents must be involved in the collection of currency cassettes, coin hoppers and/or cash boxes from kiosks and at least one agent should be independent of kiosk accountability.
3. Currency cassettes, coin hoppers, and cash boxes must be secured in a manner that restricts access to only authorized agents.
4. Redeemed vouchers collected from the kiosk must be secured and delivered to the appropriate department (cage or accounting) for reconciliation.
5. Controls must be established and procedures implemented to ensure that currency cassettes contain the correct denominations and have been properly installed. **MICS 543.17(i)**

    a) Access to stored full kiosk cash boxes, coin hoppers and currency cassettes must be restricted to:

        (1) Authorized agents; and
        (2) In an emergency, authorized persons for the resolution of a problem as outlined in the system of internal controls.

    b) The kiosk count must be performed in a secure area, such as the cage or count room.

    c) If counts from various revenue centers and kiosks occur simultaneously in the count room, procedures must be in effect that prevent the commingling of funds from the kiosks with any revenue centers.

    d) The kiosk cash boxes, coin hoppers, and currency cassettes must be individually emptied and counted so as to prevent the commingling of funds between kiosks until the count of the kiosks contents has been recorded.

        (1) The count of must be recorded in ink or other permanent form of recordation.
        (2) Coupons or other promotional items not included in gross revenue (if any) may be recorded on a supplemental document. All single-use coupons must be cancelled daily by an authorized agent to prevent improper recirculation.

    e) Procedures must be implemented to ensure that any corrections

to the count documentation are permanent, identifiable, and the original, corrected information remains legible. Corrections must be verified by two agents.

6. Controls must be established and procedures implemented to safeguard the use, access, and security of keys for kiosks.

## 13.10. Controlled Keys MICS 543.17(j)

A. Controls must be established and procedures implemented to safeguard the use, access, and security of keys in accordance with the following:

1. Each of the following requires a separate and unique key lock or alternative secure access method:
    a) Drop cabinet;
    b) Drop box release;
    c) Drop box content; and
    d) Storage racks and carts.
2. Access to and return of keys or equivalents must be documented with the date, time, and signature or other unique identifier of the agent accessing or returning the key(s).
    a) At least three (3) agents are required to be present to access and return keys.
    b) At least three (two for card game drop box keys in operations with three tables or fewer) agents are required to be present at the time count room and other count keys are issued for the count.
3. Documentation of all keys, including duplicates, must be maintained, including:
    a) Unique identifier for each individual key;
    b) Key storage location;
    c) Number of keys made, duplicated, and destroyed; and
    d) Authorization and access.
4. Custody of all keys involved in the drop and count must be maintained by a department independent of the count and the drop agents as well as those departments being dropped and counted. While preforming the drop, the Drop Team shall not be in possession of both release keys, and content keys.
    a) In the event Security acts as the drop team, the key administrator/custodian shall be precluded from access to the drop box release keys while a drop is conducted.

5. Other than the count team, no agent may have access to the drop box content keys while in possession of storage rack keys and/or release keys.
6. Other than the count team, only agents authorized to remove drop boxes are allowed access to drop box release keys.
7. Any use of keys at times other than the scheduled drop and count must be properly authorized and documented.
8. Emergency manual keys, such as an override key, for computerized, electronic, and alternative key systems must be maintained in accordance with the following:
    a) Access to the emergency manual key(s) used to access the box containing the EGM drop and count keys requires the physical involvement of at least three agents from separate departments, including management. The date, time, and reason for access, must be documented with the signatures of all participating persons signing out/in the emergency manual key(s);
    b) The custody of the emergency manual keys requires the presence of two agents from separate departments from the time of their issuance until the time of their return; and
    c) Routine physical maintenance that requires access to the emergency manual key(s), and does not involve accessing the player interface drop and count keys, only requires the presence of two agents from separate departments. The date, time, and reason for access must be documented with the signatures of all participating agents signing out/in the emergency manual key(s).

## 13.11. Variance

A. The operation must establish, as approved by the TGA, a threshold level at which variance must be reviewed to determine the cause. Any such review must be documented. **MICS 543.17(k)**

# Chapter 14 AUDITING & ACCOUNTING

## 14.1. Conflicts of Standards MICS 543.23(a)

A. When establishing SICS, the gaming operation should review, and consider incorporating, other external standards such as GAAP, GAAS, and standards promulgated by GASB and FASB. In the event of a conflict between the TICS and the incorporated external standards, the external standards prevail.

## 14.2. Signatures TSC App. A:20(1)

A. Signatures shall:

1. Be, at a minimum, the signer's first initial and last name;
2. Include his or her certificate or permit number; and
3. Signify the signer has prepared forms, and documents, and/or authorized to a sufficient extent to attest to the accuracy of the information recorded thereon, in conformity with these standards and the TGO SICS.

## 14.3. Accounting MICS 543.23(b)

A. Controls must be established and procedures implemented to safeguard assets and ensure each gaming operation:

1. Prepares accurate, complete, legible, and permanent records of all transactions pertaining to gaming revenue and activities for operational accountability.
2. Prepares general accounting records on a double-entry system of accounting, maintaining detailed, supporting, subsidiary records, and performs the following activities:
   a) Record gaming activity transactions in an accounting system to identify and track all revenues, expenses, assets, liabilities, and equity;
   b) Record all markers, IOUs, returned checks, held checks, or other similar credit instruments;
   c) Record journal entries prepared by the gaming operation and by any independent accountants used;
   d) Prepare income statements and balance sheets;
   e) Prepare appropriate subsidiary ledgers to support the balance sheet;
   f) Prepare, review, and maintain accurate financial statements;
   g) Prepare transactions in accordance with the appropriate authorization, as provided by management;
   h) Record transactions to facilitate proper recording of gaming

revenue and fees, and to maintain accountability of assets;

i) Compare recorded accountability for assets to actual assets at periodic intervals, and take appropriate action with respect to any variances;

j) Segregate functions, duties, and responsibilities;

k) Prepare minimum bankroll calculations; and

l) Maintain and preserve all financial records and relevant supporting documentation.

## 14.4. Internal Audit MICS 543.23(c)

A. Internal auditor(s) perform audits of each department of a gaming operation, at least annually, to review compliance with the TICS, SICS, MICS, and the Tribal State Compact which include at least the following areas:

1. Bingo, including supervision, bingo cards, bingo card sales, draw, prize payout; cash and equivalent controls, technologic aids to the play of bingo, operations, vouchers, and revenue audit procedures;
2. Card games, including supervision, exchange or transfers, playing cards, shill funds, reconciliation of card room bank, posted rules, and promotional progressive pots and pools;
3. Gaming promotions and player tracking procedures, including supervision, gaming promotion rules and player tracking systems **MICS 543.23(c)(1)(iv)**;
4. Complimentary services or items, including procedures for issuing, authorizing, redeeming, and reporting complimentary service items;
5. Patron deposit accounts and cashless system procedures, including supervision, patron deposit accounts and cashless systems, as well as patron deposits, withdrawals and adjustments;
6. Lines of credit procedures, including establishment of lines of credit policy;
7. Drop and count standards, including supervision, count room access, count team, card game drop standards, player interface and financial instrument drop standards, card game count standards, player interface financial instrument count standards, collecting currency cassettes and financial instrument storage components from kiosks, kiosk count standards, and controlled keys;
8. Cage, vault, cash and cash equivalent procedures, including supervision, cash and cash equivalents, personal checks, cashier's checks, traveler's checks, payroll checks, and counter checks, cage and vault accountability, kiosks, patron deposited funds, promotional payouts, drawings, and giveaway programs, chip and token standards, and cage and vault access;

9. Information technology, including supervision, gaming systems' logical and physical controls, independence, physical security, logical security, user controls, installations and/or modifications, remote access, incident monitoring and reporting, data back-ups, software downloads, and verifying downloads; and
10. Accounting standards, including accounting records, maintenance and preservation of financial records and relevant supporting documentation.

B. Internal auditor(s) are independent of gaming operations with respect to the departments subject to audit.

C. Internal auditor(s) report directly to the Tribe, or other entity designated by the Tribe.

D. Documentation such as checklists, programs, reports, etc. is prepared to evidence all internal audit work and follow-up performed as it relates to the requirements in this section, including all instances of noncompliance.

E. Audit reports are maintained and made available to the NIGC upon request and must include the following information:
1. Audit objectives;
2. Audit procedures and scope;
3. Findings and conclusions **MICS 543.23(c)(5)(iii)**;
4. Recommendations, if applicable; and
5. Management's response.

F. All material exceptions identified by internal audit work are investigated and resolved and the results are documented.

G. Internal audit findings are reported to management, responded to by management stating corrective measures to be taken, and included in the report delivered to management, the Tribe, TGA, audit committee, or other entity designated by the Tribe for corrective action.

H. Follow-up observations and examinations is performed to verify that corrective action has been taken regarding all instances of non-compliance. The verification is performed within six (6) months following the date of notification of non-compliance.

## 14.5. Annual Requirements MICS 542.23(d)

A. Agreed upon procedures. A CPA must be engaged to perform an independent assessment to verify whether the gaming operation is in compliance with the MICS, and/or the TICS or SICS if they provide at least the same level of controls as the MICS. The independent assessment must be performed in accordance with agreed upon procedures and the most recent versions of the Statements on

Standards for Attestation Engagements and Agreed-Upon Procedures Engagements (collectively "SSAEs"), issued by the American Institute of Certified Public Accountants.

B. The TGO must submit two copies of the agreed-upon procedures report to TGA, WSGC, and NIGC within 120 days of the gaming operation's fiscal year end in conjunction with the submission of the annual financial audit report required pursuant to TSC and 25 CFR part 571.

C. Review of internal audit

1. The CPA must determine compliance by the gaming operation with the internal audit requirements in this section by:

a) Completing the internal audit checklist;

b) Ensuring that the internal auditor completed checklists for each gaming department of the operation;

c) Verifying that any areas of non-compliance have been identified;

d) Ensuring that audit reports are completed and include responses from management; and

e) Verifying that appropriate follow-up on audit findings has been conducted and necessary corrective measures have been taken to effectively mitigate the noted risks.

2. If the CPA determines that the internal audit procedures performed during the fiscal year have been properly completed, the CPA may rely on the work of the internal audit for the completion of the MICS checklists as they relate to the standards covered by this part.

D. Report format. The SSAEs are applicable to agreed-upon procedures engagements required in this part. All noted instances of noncompliance with the MICS and/or the TICS or SICS, if they provide the same level of controls as the MICS, must be documented in the report with a narrative description, the number of exceptions and sample size tested.

# Chapter 15 AUDITING REVENUE

## 15.1. Supervision MICS 543.24(a)

A. Supervision must be provided as required for operations by an agent(s) with authority greater than those being supervised.

## 15.2. Independence MICS 543.24(b)

A. Audits must be performed by agent(s) independent of the transactions being audited.

## 15.3. Documentation MICS 543.24(c)

A. The performance of revenue audit procedures, the exceptions noted, and the follow-up of all revenue audit exceptions must be documented and maintained.

## 15.4. Controls

A. Bingo MICS 543.24(d)(1)

1. At the end of each month, verify the accuracy of the ending balance in the bingo control log by reconciling it with the bingo paper inventory. Investigate and document any variance noted.
2. Daily, reconcile supporting records and documents to summarized paperwork or electronic records (e.g. total sales and payouts per shift and/or day).
3. At least monthly, review variances related to bingo accounting data in accordance with an established threshold, which must include, at a minimum, variance(s) noted by the gaming system for cashless transactions in and out, electronic funds transfer in and out, external bonus payouts, vouchers out and coupon promotion out. Investigate and document any variance noted.
4. At least monthly, review statistical reports for any deviations from the mathematical expectations exceeding a threshold established by the TGA. Investigate and document any deviations compared to the mathematical expectations required to be submitted per **MICS 547.4**.
5. At least monthly, take a random sample, foot the vouchers redeemed and trace the totals to the totals recorded in the voucher system and to the amount recorded in the applicable cashier's accountability document.

B. Card Games MICS 543.24(d)(3)

1. Daily, reconcile the amount indicated on the progressive sign/meter to the cash counted or received by the cage and the payouts made for each promotional progressive pot and pool. This reconciliation must be sufficiently documented, including substantiation of differences and

adjustments.

2. At least monthly, review all payouts for the promotional progressive pots, pools, or other promotions to verify payout accuracy and proper accounting treatment and that they are conducted in accordance with conditions provided to the patrons.

3. At the conclusion of each contest/tournament, reconcile all contest/tournament entry and payout forms to the dollar amounts recorded in the appropriate accountability document.

C. Gaming Promotions and Player Tracking MICS 543.24(d)(4)

1. At least monthly, review promotional payments, drawings, and giveaway programs to verify payout accuracy and proper accounting treatment in accordance with the rules provided to patrons.

2. At least monthly, for computerized player tracking systems, perform the following procedures:

   a) Review authorization documentation for all manual point additions/deletions for propriety;

   b) Review exception reports, including transfers between accounts; and

   c) Review documentation related to access to inactive and closed accounts.

3. At least annually, all computerized player tracking systems must be reviewed by agent(s) independent of the individuals that set up or make changes to the system parameters. The review must be performed to determine that the configuration parameters are accurate and have not been altered without appropriate management authorization Document and maintain the test results.

D. Patron Deposit Accounts MICS 542.24(d)(6)

1. At least weekly, reconcile patron deposit account liability (deposits ±adjustments−withdrawals = total account balance) to the system record.

2. At least weekly, review manual increases and decreases to/from player deposit accounts to ensure proper adjustments were authorized.

E. Lines of Credit MICS 542.24(d)(7)

1. At least three (3) times per year, an agent independent of the cage, credit, and collection functions must perform the following review:

a) Select a sample of line of credit accounts;

b) Ascertain compliance with credit limits and other established credit issuance procedures;

c) Reconcile outstanding balances of both active and inactive (includes write-offs and settlements) accounts on the accounts receivable listing to individual credit records and physical instruments. This procedure need only be performed once per year for inactive accounts; and

d) Examine line of credit records to determine that appropriate collection efforts are being made and payments are being properly recorded.

e) For at least five (5) days during the review period, subsequently reconcile partial payment receipts to the total payments recorded by the cage for the day and account for the receipts numerically.

2. At least monthly, perform an evaluation of the collection percentage of credit issued to identify unusual trends.

F. Complimentary Services or Items. MICS 543.24(d)(5)

1. At least monthly, review the complimentary services and items report for proper authorization and compliance with established authorization thresholds. These reports must be made available to those entities authorized by TGA or by tribal law or ordinance.

G. Drop and Count MICS 543.24(d)(8)

1. At least quarterly, unannounced currency counter and currency counter interface (if applicable) tests must be performed, and the test results documented and maintained. All denominations of currency and all types of cash out tickets counted by the currency counter must be tested. This test may be performed by internal audit or TGA. The result of these tests must be documented and signed by the agent(s) performing the test.

2. At least quarterly, unannounced weigh scale and weigh scale interface (if applicable) tests must be performed, and the test results documented and maintained. This test may be performed by internal audit or the TGA. The result of these tests must be documented and signed by the agent(s) performing the test.

3. For computerized key security systems controlling access to drop and count keys, perform the following procedures:

a) At least quarterly, review the report generated by the computerized key security system indicating the transactions performed by the individual(s) that adds, deletes, and changes users' access within the system (i.e., system administrator). Determine whether the transactions completed by the system administrator provide adequate control over the access to the drop and count keys. Also, determine whether any drop and count key(s) removed or returned to the key cabinet by the system administrator was properly authorized;

b) At least quarterly, review the report generated by the computerized key security system indicating all transactions performed to determine whether any unusual drop and count key removals or key returns occurred; and

c) At least quarterly, review a sample of users that are assigned access to the drop and count keys to determine that their access to the assigned keys is appropriate relative to their job position.

4. At least quarterly, an inventory of all controlled keys must be performed and reconciled to records of keys made, issued, and destroyed. Investigations must be performed for all keys unaccounted for, and the investigation documented.

H. Cage, Vault, Cash, and Cash Equivalents MICS 543.24(d)(8)

1. At least monthly, the cage accountability must be reconciled to the general ledger.

2. At least monthly, trace the amount of cage deposits to the amounts indicated in the bank statements.

3. Twice annually, a count must be performed of all funds in all gaming areas (i.e. cages, vaults, and booths (including reserve areas), kiosks, cash-out ticket redemption machines, and change machines. Count all chips and tokens by denomination and type. Count individual straps, bags, and imprest banks on a sample basis. Reconcile all amounts counted to the amounts recorded on the corresponding accountability forms to ensure that the proper amounts are recorded. Maintain documentation evidencing the amount counted for each area and the subsequent comparison to the corresponding accountability form. The count must be completed within the same gaming day for all areas.

a) Counts must be observed by an individual independent of the department being counted. It is permissible for the individual responsible for the funds to perform the actual count while being observed.

b) Internal audit may perform and/or observe the two counts.

4. At least annually, select a sample of invoices for chips and tokens

purchased, and trace the dollar amount from the purchase invoice to the accountability document that indicates the increase to the chip or token inventory to ensure that the proper dollar amount has been recorded.

5. At each business year end, create and maintain documentation evidencing the amount of the chip/token liability, the change in the liability from the previous year, and explanations for adjustments to the liability account including any adjustments for chip/token float.
6. At least monthly, review a sample of returned checks to determine that the required information was recorded by cage agent(s) when the check was cashed.
7. At least monthly, review exception reports for all computerized cage systems for propriety of transactions and unusual occurrences. The review must include, but is not limited to, voided authorizations. All noted improper transactions or unusual occurrences identified must be investigated and the results documented.
8. Daily, reconcile all parts of forms used to document increases/decreases to the total cage inventory, investigate any variances noted, and document the results of such investigations.

I. Electronic Gaming Machine MICS 542.13(m)

1. Electronic game accounting/auditing procedures shall be performed by employees who are independent of the transactions being reviewed
2. Procedures shall be performed at least monthly to verify that the Player Account Server is transmitting and receiving data properly and to verify the continuing accuracy of the ticket-in meter readings as recorded in the statistical reports.
3. For each drop period, accounting/auditing personnel shall compare the bill-in meter reading to the actual drop amount. Discrepancies should be resolved prior to generation/distribution of statistical reports
4. Follow-up shall be performed for any one machine having an unresolved variance between actual drop and bill-in meter reading in excess of 3%. The follow-up performed and results of the investigation shall be documented and maintained.
5. At least weekly, accounting/auditing employees shall compare the bill-in meter reading to the total currency acceptor drop amount for the week. Discrepancies shall be resolved prior to the generation/distribution of electronic game statistical reports.
6. TGA shall be immediately notified of the existence of any unresolved variance.
7. The follow-up performed and results of the investigation shall be documented and maintained for inspection by TGA.

8. At least annually, accounting/auditing personnel shall randomly verify that EPROM or other equivalent game software media changes are properly reflected in the gaming machine analysis reports.
9. Accounting/auditing employees shall review exception reports for all computerized electronic game systems on a daily basis for propriety of transactions and unusual occurrences.
10. All electronic game auditing procedures and any follow-up performed shall be documented and maintained for inspection.

J. Table Games MICS 542.12(j)

1. The accounting and auditing procedures shall be performed by personnel who are independent of the transactions being audited/accounted for.
2. If a table game has the capability to determine drop, the dollar amount of the drop shall be reconciled to the actual drop by shift.
3. Accounting/auditing employees shall review exception reports for all computerized table games systems at least monthly for propriety of transactions and unusual occurrences.
4. All noted improper transactions or unusual occurrences shall be investigated with the results documented.
5. Evidence of table games auditing procedures and any follow-up performed shall be documented, maintained for inspection, and provided to TGA upon request.
6. A daily recap shall be prepared for the day and month-to-date, which shall include the following information:
    a) Drop;
    b) Win, and
    c) Gross revenue.

# Chapter 16 PROGRESSIVE JACKPOT STANDARDS

## 16.1. Defining Progressive Jackpot also known as "player-supported jackpot."

A. "Player-supported jackpot" (PSJ) means a separate contest of chance directly related to the play or outcome of an authorized Table Game, Tribal Lottery System, or Electronic Bingo game.

1. In PSJs, operations:

a) Collect funds from the players' wagers (the pot) for a separate prize; and

b) Act only as the custodian of the PSJ funds, including any interest earned on this money; and

c) Maintain no legal right to the funds, except for administrative fees; and

d) Must strictly account for all funds.

## 16.2. Getting approval for player-supported jackpots

A. To get a PSJ approved, operations must make a written request, including, at least:

a) For Table Games, a detailed description of the game associated with the PSJ; and

b) All internal control procedures associated with the PSJ and accounting for funds and prizes; and

c) The name of the prize fund custodian.

B. Operations must get Tribal Gaming Agency written approval before making any changes to the PSJ.

## 16.3. Naming a prize fund custodian for a player-supported jackpot

A. Operations must identify the prize fund custodian by position who is responsible and accountable for safeguarding player-supported jackpot funds, and for disbursing funds to winners.

## 16.4. Posting rules for a player-supported jackpot

A. Operations must provide a pamphlet or prominently post a sign stating:

1. How they will distribute player supported jackpot (PSJ) money if they discontinue the PSJ or stop operating the game; and

2. Conditions under which prizes may be won; and

3. Prize amount; and

4. Cost to participate; and
5. Administrative fees; and
6. Any other conditions which may affect the outcome of the game.

## 16.5. Seeding a player-supported jackpot

A. Operations may:
   1. Seed a PSJ and replenish the PSJ when depleted; and
   2. Recover seed money.

## 16.6. Collecting funds for a player-supported jackpot

A. Operations may collect funds from the pot for each player-supported jackpot.
   1. Operations must keep these funds separate from all other fees.

## 16.7. Collecting an administrative fee on the player-supported jackpot

A. Operations may collect an administrative fee of up to ten percent of the funds collected for a player supported jackpot (PSJ). Operations must deduct no other expenses from the PSJ account.

## 16.8. Accounting for player-supported jackpot funds.

A. Operations must:
   1. Maintain a separate accounting fund for holding player-supported jackpot (PSJ) funds; and
   2. Deposit only funds from PSJs into the account; and
   3. Identify all deposits or transfers of PSJ funds by the type of PSJ fund and date of collection; and
   4. Transfer the amount from the PSJ account to the cage or general account before the end of the month if PSJ prizes are paid from the cage or general account. The licensee must keep the transfer information as part of the written records; and
   5. Reconcile the account balance in the progressive meters to the PSJ prize balance on the PSJ prize fund accrual record each month. "Reconcile" means the licensee operation must compare the two balances, resolve any differences, and document the comparison and the differences in writing. Operations must keep the reconciliation as part of their records.
   6. Any unresolved variances shall be reported to the Tribal Gaming Agency with seven (7) days.

## 16.9. Paying out prizes on a player-supported jackpot.

A. Operations must award all player-supported jackpot funds as prizes; and

B. Prizes of five thousand dollars or less may be paid in cash or chips; and

C. Prizes not awarded at the time of PSJ win must be paid within twenty-four hours with a check that provides a duplicate copy; and

D. Operations must maintain a record of all prizes paid.

## 16.10. Removing a player-supported jackpot from play.

A. If Operations discontinue a PSJ, they must distribute the balance, less any seed money, to players within thirty days by offering an approved promotion or tournament of the same game played to fund the PSJ.

## 16.11. Resolving disputes over player-supported jackpots.

A. If a dispute arises involving the outcome of a player-supported jackpot (PSJ), Operations must:

1. Preserve the video recording and all records for the game where the dispute occurred; and
2. Document all information about the dispute, including:
    a) The names, addresses, and phone numbers of all players, staff, and any witnesses involved; and
    b) The amount of the advertised PSJ; and
    c) A full description of the circumstances surrounding the dispute; and
3. Notify the Tribal Gaming Agency immediately of any unresolved player disputes.

B. The Tribal Gaming Agency will investigate complaints involving PSJ disputes and may issue a written decision which is final.

C. Operation must not award or advertise the prize amount which is in dispute until it is resolved.

# Chapter 17 TITLE 31 COMPLIANCE

## 17.1. Reports of Transactions in Currency 31 CFR 1021.310

A. A report of each transaction in currency involving either cash-in or cash-out of more than $10,000 must be filed with FinCEN.

B. Multiple currency transactions are treated as a single transaction if the gaming operation has knowledge that the multiple currency transactions are by or on behalf of any person and result in either cash-in or cash-out totaling more than $10,000 during any gaming day.

1. Knowledge is deemed to exist if any manager, director, or employee of the gaming operations, acting within the scope of his or her employment, has knowledge that such multiple currency transactions have occurred.

2. Knowledge also includes that obtained from examining information recorded on books, records, logs, magnetic disk/tape/machine-readable media, and information maintained by the gaming operations pursuant to any law or regulation or within the ordinary course of its business, and which contain information that such multiple currency transactions have occurred.

## 17.2. Reports of Suspicious Transactions 31 CFR 1021.320

A. A report of any suspicious transaction relevant to a possible violation of law or regulation must be filed with FinCEN. This includes any suspicious transaction that is believed relevant to the possible violation of any law or regulation but whose reporting is not required because of its dollar amount.

B. A transaction is suspicious if it is conducted or attempted by, at, or through a gaming operation and involves aggregates at least $5,000 in funds or other assets, and the gaming operation knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part):

1. Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;

2. Is designed, whether through structuring or any other means, to evade any requirements any regulations promulgated under the Bank Secrecy Act; or

3. Has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the gaming operation knows of no reasonable explanation for the transaction

after examining the available facts, including the background and possible purpose of the transaction.

C. Reports of suspicious activity (Suspicious Activity Reports by Casinos, a.k.a. SARC's) are to be filed with FinCEN no later than 30 calendar days after the date of the initial detection of facts that may constitute a basis for possible violation of law or regulation. If no suspect is identified on the date of such initial detection, a delay of an additional 30 calendar days is permitted. In no case shall reporting be delayed by more than 60 calendar days after the initial detection. In situations involving violations that require immediate attention, such as ongoing money laundering schemes, the gaming operation shall immediately notify by telephone an appropriate law enforcement authority in addition to filing the SARC.

D. The gaming operation shall maintain a copy of any SARC filed and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SARC. Supporting documentation shall be identified as such and maintained by the gaming operation and shall be deemed to have been filed with the SARC.

E. The gaming operation shall make all supporting documentation available to FinCEN and any other appropriate law enforcement agencies or federal, state, local, or tribal gaming regulators upon request.

F. No director, employee, or agent of the gaming operation who has reported a suspicious transaction may notify any person involved in the transaction that the transaction has been reported. Any subpoena or request to disclose a SARC or the information contained in a SARC, other than by FinCEN or another appropriate law enforcement or regulatory agency, shall be declined to include any information that a SARC has been prepared or filed. FinCEN shall be informed of any such request and the response given to such a request.

## 17.3. Filing of Reports 31 CFR 1021.311

A. Reports of Transactions in Currency shall be filed within 15 days following the day on which the reportable transaction occurred.

B. A copy of each report filed shall be retained for a period of five years form the date of the report.

C. All reports required to be filed shall be filed with the Commissioner of Internal Revenue, unless otherwise specified.

D. Reports required shall be filed on forms prescribed by the Secretary of the Treasury. All information called for in such forms shall be furnished.

E. Forms to be used in making the reports required may be obtained from the Internal Revenue Service.

## 17.4. Identification Required 31 CFR 1021.312

A. Before concluding any transaction with respect to which a report is required, the name and address of the individual presenting a transaction shall be verified and recorded. Also recorded shall be the identity, account number, and the social security or taxpayer identification number, if any, of any person on whose behalf such transaction is to be effected.

B. Verification of the identity of an individual who indicates that he or she is an alien or is not a resident of the United States must be made by passport, alien identification card, or other official document evidencing nationality or residence (e.g., a Provincial driver's license with indication of home address).

C. Verification of identity in any other case shall be made by examination of a document that is normally acceptable as a means of identification e.g., a driver's license.

D. In each instance, the specific identifying information (i.e., the driver's license number, passport number, etc.) used in verifying the identity of the customer shall be recorded on the report. Mere notation of "known customer" or "player tracking info on file" on the report is prohibited.

## 17.5. Records to be Made and Retained 31 CFR 1021.400-410

A. Each gaming operation shall retain either the original or a microfilm or other copy or reproduction of each of the following:

B. All records, documents, or manuals required to be maintained by regulations of NIGC, WSGC, or TGA.

C. All records that are prepared or used by a gaming operation to monitor a customer's gaming activity.

D. A separate record containing a list of each transaction between the gaming operation and its customers involving any monetary instruments having a face value of $3,000 or more. Applicable transactions will be placed on the list in the chronological order in which they occur. This list will contain:

1. The time, date, and amount of the transaction;
2. The name and permanent address of the customer;
3. The type of instrument;
4. The name of the drawee or issuer of the instrument;
5. All reference numbers of the instrument; and
6. The name and license number of the gaming operation employee who conducted the transaction.

E. A copy of the Compliance Program described below. 31 CFR1021.210(b)

## 17.6. Nature of Records and Retention Period 31 CFR 1010.410

A. Wherever it is required that there be retained either the original or a microfilm or other copy or reproduction of a monetary instrument, there shall be retained a copy of both front and back of each such instrument or document, except that no copy need be retained of the back of any instrument or document which is entirely blank or which contains only standardized printed information, a copy of which is on file.

B. All records that are required to be retained shall be retained for a period of five years.

C. All such records shall be filed or stored in such a way as to be accessible within a reasonable period of time, taking into consideration the nature of the records, and the amount of time expired since the record was made.

## 17.7. Structuring Transactions 31 CFR 1010.314

A. No person shall for the purpose of evading the reporting requirements of these regulations with respect to each such transaction:

1. Cause or attempt to cause the gaming operation to fail to file a report required under Title 31.
2. Cause or attempt to cause a gaming operation to file a report required under Title 31 that contains a material omission or misstatement of fact; or
3. Structure or assist in structuring, or attempt to structure or assist in structuring, in any manner, any transaction for the purpose of evading the reporting requirements of Title 31.

## 17.8. Compliance Program 31 CFR1021.210(b)

A. Each gaming operation shall develop and implement a written program reasonably designed to assure and monitor compliance with the requirements of Title 31.

B. At a minimum, each compliance program shall provide for:

1. A system of internal controls to assure ongoing compliance;
2. Annual internal and/or external independent testing of compliance, including, without limitation, an annual statement whether internal controls and procedures are working effectively to detect and report suspicious transactions of $5,000 or more, and currency transaction of more than $10,000, to the proper authorities, as required by Title 31, and to comply with the record keeping and compliance program standards of this part.
3. Training of gaming operations personnel, including training in the

identification of unusual or suspicious transactions

4. An individual or individuals to assure day-to-day compliance;
5. Procedures for using all available information to determine:
    a) When required, the name, address, social security number, and other information and verification of the same, of a person;
    b) The occurrence of any transactions or patterns of transactions required to be reported including, without limitation, any transactions or patterns of transactions indicated by accounts or records maintained by the gaming operation to record or monitor customer activity.
    c) Whether any record as described must be made and retained; and
6. For gaming operations that have automated data processing systems, the use of automated programs to aid in assuring compliance.

# Chapter 18 KENO

The following definitions apply to this Chapter only.

## 18.1. Keno Definitions

A. Ball Draw Equipment means any mechanical device, apparatus, or equipment which facilitates the random selection of numbered Keno balls.

B. Game Grid means the consecutively numbered field from one (1) to eighty (80) numbers on which Winning Numbers and Winning Plays are designated.

C. Informational Materials means printed materials explaining rules of play; prizes; deadlines for redeeming prizes; and rules concerning splitting of prizes when necessary.

D. Inside Ticket means a form on which the players indicate their selections, which may include a request for a Quick Pick Selection to be issued through the use of a Quick Pick Device.

E. Keno means a numbers game where players choose from one to ten numbers out of a pool of eighty and winners are determined by correctly matching selected numbers to twenty randomly selected numbers.

F. Keno Manager means the person responsible for controlling Keno department operations, who safeguards Keno assets and ensures compliance with applicable laws and regulations. Shares the duty of approving payouts of $4,000.00 or more with the Casino Shift Manager.

G. Keno Runner means any person authorized by the Tribal Gaming Agency to accept completed Inside Tickets, and the prices thereof, and to return Outside Tickets and prizes won, acting as an agent of the player.

H. Keno Shift Manager means the person responsible for all Keno department operations during his or her assigned shift.

I. Keno Shift Supervisor means the person who in the absence of the Keno Shift Manager is responsible for all Keno department operations during his or her assigned shift.

J. Keno System means the collection of hardware and software components which facilitate the play, reporting, and security of the Keno game. The Keno System includes: number selection devices, databases, servers, networking devices, management terminals, kiosks, and other components used as integral parts of the Keno game

K. Keno Writer means a person who operates the Random Number Generator authorized by the Tribal Gaming Agency to select Winning Numbers for each game, and is also authorized by the Tribal Gaming Agency to validate completed

Inside Tickets, verify and accept the authorized price thereof, issue Outside Tickets and Quick Pick Tickets, and make payments for winning Outside Tickets.

L. Kiosk means an employee staffed computer or device, where Keno tickets may be purchased or redeemed.

M. Number or Spot means any of the numbers on the Game Grid.

N. Outside Ticket means the computer generated and printed form which indicates the numbers selected and conditions of the wager made by a player on an Inside Ticket, which may be a Quick Pick Selection.

O. Play means a selection of one or more groups of up to twenty (20) numbers in one (1) to twenty-six (26) groups. No Play or wager shall be deemed made until an Outside Ticket has been issued by a Keno Writer in receipt for an Inside Ticket and the prices of Plays indicated thereon.

P. Promotional Prize means a prize established by management and approved by the Tribal Gaming Agency for promotional purposes, and which deviates from the Standard Prize.

Q. Quick Pick Device means a Random Number Generator authorized by the Tribal Gaming Agency for making Quick Pick Selections.

R. Quick Pick Selection means any Play made through the use of a Quick Pick Device.

S. Quick Pick Ticket means the form of an Outside Ticket designated by the Tribal Gaming Agency issued through the use of a Quick Pick Device.

T. Rabbit Ears means a device, generally V-shaped, that is attached to the Keno blower and holds the numbered balls selected during a Keno game so that the numbers are visible to players and employees.

U. Random Number Generator means a hardware or software component which randomly generates Keno numbers.

V. Standard Prize means the standard prizes established by management and approved by the Tribal Gaming Agency for matching a required quantity of player or quick pick selected numbers with Winning Numbers in any given game.

W. Ticket means a physical ticket issued to a player which includes applicable game play and wagering information.

X. Transaction Log means a record of the information printed on each ticket which is either recorded electronically by the system or printed out physically.

Y. Win means prizes paid.

Z. Winning Numbers means the twenty (20) numbers, from one (1) to eighty (80), which are randomly selected for each game.

AA. Winning Plays means those combinations of numbers entitled to Standard Prizes or Promotional Prizes.

BB. Write means gross revenue from Keno ticket sales.

CC. Writer means Keno employee who staffs a Kiosk.

DD. Way means a Play when more than one Play is made on the same Inside Ticket.

## 18.2. Rules of Play

A. Twenty (20) numbers are randomly drawn by the house for each game. The game is played by matching players' numbers with those drawn by the house. Predetermined prizes are awarded based on how many matching numbers are drawn.

B. Players make Plays by directly marking their selections on an Inside Ticket, requesting a Quick Pick Selection or by requesting the replay of an Outside Ticket from a previous game.

C. The player's Inside Ticket must be validated by a Keno Writer and paid for before it is placed in play. No Play shall be deemed made until an Outside Ticket verifying the validity of and receipt of the authorized price for the Inside Ticket has been issued by a Keno Writer. No Play may be validated after a Keno Writer declares the game closed. All games shall be closed at least five (5) seconds before the Winning Numbers are selected.

D. The game is played when and where the Outside Tickets are validated by a Keno Writer, and shall be deemed completed when a Keno Writer selects the twentieth (20) Winning Number. All selections of Winning Numbers by a Keno Writer shall be conducted in full view of the public. All numbers selected will be prominently displayed immediately upon selection.

E. A Winning Play is achieved when the Play results in a quantity of player or Quick Pick selected Numbers matching Winning Numbers which have been drawn for that game. Management shall publish in the Informational Materials a Standard Prize schedule, and any Promotional Prizes to be offered, as approved by the Tribal Gaming Agency.

F. After selection of the twentieth (20) Winning Number, the Keno Shift Manager or Keno Shift Supervisor will verify the numbers drawn for the game and authorize payment of prizes due in connection therewith. The Keno Manager or Casino Shift Manager will personally authorize payments of all prizes of $4,000.00 and over. Unless otherwise specified by the Tribal Gaming Agency prior to the game, winning Outside Tickets which are not submitted for verification within five (5) games of the last game number shown on the Outside Ticket shall be void, and any prize to which the holder of such Outside Ticket would have been entitled shall be forfeited.

G. Any player who claims to have won a prize must present a validated Outside Ticket to a Keno Writer. In addition, the claimant may be required to complete a claim form and submit it prior to validation and payment. The apparent winning Outside Ticket must be presented in person, or through the services of a Keno Runner acting as the player's agent. In addition, a player may be required to complete any applicable tax forms prior to receiving payment, which may be subject to the deduction of withholding taxes.

H. A Keno Writer will promptly present the prize to the claimant in payment of the amount due, less any withholding required, or will notify the claimant that the Outside Ticket is not a Winning Play, is not entitled to a prize, and that the claim is denied. Non-winning Outside Tickets may be retained by management, and not returned to the claimant.

## 18.3. Tickets

A. Players select the numbers they wish to play on the form provided (Inside Ticket) and purchase a ticket from a kiosk (Outside Ticket).

B. The Outside Ticket includes the numbers selected, date, game number, conditioning, ticket sequence number and the kiosk number.

C. Matching information from the ticket is written concurrently to the Transaction log.

D. When it is necessary to void a ticket, the void information is input into the system which documents the appropriate information pertaining to the voided wager (e.g., void slip is issued or equivalent documentation is generated).

E. Physical and operational controls should prevent the writing and voiding of tickets after a game has been closed and after the number selection process has begun.

F. Copies of all Keno tickets shall be maintained for at least 7 days.

## 18.4. Price of Play

A. The price of each Play shall be established by management and approved by the Tribal Gaming Agency. The total cost for purchasing an Outside Ticket shall equal the sum of prices for all Plays designated on the Inside Ticket. Management may, but shall not be required to, offer special prices for Promotional Plays and Ways, as approved by the Tribal Gaming Agency.

## 18.5. Prizes

A. The prize amounts to be paid to each player who selects a winning combination of numbers shall be determined by management as approved by the Tribal Gaming Agency, and the prize structure may vary from time to time. There shall be a basic or Standard Prize schedule. From time to time, management as

approved by the Tribal Gaming Agency may create Promotional Prize structures. Payment of all prizes will be in compliance with the requirements of Section 2 above.

B. A Winning Play shall only be entitled to the greatest available prize for such Play. Lesser included Winning Plays within such Play shall not be awarded prizes.

C. In determining Standard and Promotional Prizes, management as approved by the Tribal Gaming Agency may declare, in advance of any game, that multiple winners for identical Winning Plays shall split the prizes for such Plays. In such cases, the condition that such prizes will be split shall be printed on the Inside Tickets for such games and in any Informational Materials distributed to players in connection therewith.

D. Prize schedules will be posted in a conspicuous location, in the vicinity of the place where a Keno Writer selects the Winning Numbers, and shall be available through the Informational Materials which shall be made available to players upon request before any game is played.

## 18.6. Drawings of Winning Numbers

A. Drawings of Winning Numbers will be conducted in the location and at the times designated by management as approved by the Tribal Gaming Agency. Management as approved by the Tribal Gaming Agency may change the drawing schedule or cancel drawings at any time. Winning Numbers are not official until verified by the Keno Shift Manager or Keno Shift Supervisor.

B. The Tribal Gaming Agency shall approve the type of equipment to be used, shall establish procedures for its operation and security, and shall establish the procedures for randomly selecting the Winning Numbers for each game.

1. The selected numbers using Ball Drop Equipment shall be immediately entered in the System by Keno personnel or other method approved by TGA and SGA, which documents on a draw ticket the date, game number, the time the game was closed, and the numbers drawn.
2. Alternatively, when a Random Number Generator is used, it will be linked to the System and will directly record the Numbers selected into the System. The Random Number Generators used shall be periodically tested to assure proper operation, security, and lack of tampering or fraud.
3. Physical and operational controls shall prevent the modification of the numbers drawn for each game.

C. The Keno Shift Manager or Keno Shift-Supervisor shall delay payment of all prizes in connection with any game for which any evidence exists or there are grounds for suspicion that tampering or fraud has occurred. In such instances, payment of prizes shall only be made after an authorized agent of the Tribal

Gaming Agency completes an investigation. If the drawing cannot be verified as being free from fraud or tampering, no prizes will be awarded and another drawing may be conducted in its place to determine the Winning Numbers for the questioned game.

## 18.7. Verification Requirements and Controls

A. To be verified as a valid winning Outside Ticket, all of the following conditions must be met:

1. All payouts shall be supported by the customer copy of the winning ticket (Outside Ticket) and the payout amount is indicated on the customer ticket or a payment slip is issued.
2. The Outside Ticket shall be intact, contain all printing in its entirety, be legible, and correspond to the serial number or other verifying identification issued by the Keno Writer before the game began.
3. The Outside Ticket shall not be mutilated, altered, or tampered with in any manner, and shall not be counterfeit or a facsimile of another winning Outside Ticket.
4. The Outside Ticket shall be validated by a Keno Writer, in an authorized manner. The System shall prevent payment on tickets previously presented for payment, unclaimed Winning Tickets (sleepers) after a specified period of time, voided Tickets, and Tickets which have not been issued yet.
5. The Outside Ticket shall pass all other confidential security checks of management or the Tribal Gaming Agency.
6. Larger Prize Report. A report will be required for all prizes that exceed the threshold that triggers additional procedures to be followed for the purposes of compliance with federal tax reporting requirements. At a minimum, on a daily and monthly basis, the report shall provide the date and time won and the amount of all prizes

B. Any Outside Ticket failing any verification requirement listed above is invalid, not eligible for a prize, and not subject to any refund.

C. Management, as approved by the Tribal Gaming Agency may, at its option, replace an invalid Outside Ticket with another Outside Ticket of equivalent value for a future drawing of the game. Management as approved by the Tribal Gaming Agency may, at its option, pay the prize for an Outside Ticket that is partially mutilated or is not intact if the Outside Ticket can still be validated by other means.

D. In the event an Outside Ticket is issued in error or is defective, the only responsibility or liability of management or the Tribe shall be the replacement of the erroneous or defective Outside Ticket with another Outside Ticket of

equivalent value for a future drawing.

E. The play of Keno will be subject to the same type of internal controls, including periodic audits and documentation to create a paper trail, as is established by the Tribal Gaming Agency for other Class III Gaming.

## 18.8. Reports

A. Records shall be maintained which include Win and Write by individual writer for each shift.

B. Records shall be maintained which include Win, Write, and Win-to-Write hold percentage for:

1. Each shift;
2. Each day;
3. Month-to-date;
4. Year-to-date.

C. The system shall provide at a minimum the following reports:

1. Ticket information.
2. Payout information.
3. Game information including game number, ball draw, date, and time.
4. System exception reports, including:
   a) Voids.
   b) Late pays.
   c) Appropriate system parameter information.

## 18.9. System Security Standards

A. Physical and operational controls must be in place to ensure access to Keno System and its components are restricted to authorized users and shall prevent the modification of game information.

B. Back-up Keno ball inventories shall be secured in a manner to prevent unauthorized access. Controls must be established for inspecting new Keno balls put into play as well as for those in use.

C. Each authorized user must have a user name or number unique to that individual and must access the Keno System software by means of a password, keycard, PIN number, or other unique identifier. The System must log the date and time of each access. These access logs must be available for audit by TGA and SGA.

D. Except for kiosks, all main System components including servers and networking equipment shall at a minimum be enclosed in a locked and monitored cabinet. Access shall be through the use of access controls defined in E below.

E. Keys which provide access to any locked compartment, component or area of the Keno System, as well as passwords, keycards, or PIN numbers used to access Keno System components, shall be maintained and used in accordance with the access control standards as agreed to by TGA and SGA.

F. Networking Standards

1. All Keno System components shall be hardwired within a dedicated network and located within the gaming facility.
2. Communications between all components of the Keno System must be encrypted utilizing a minimum of Data Encryption Standards (DES) or equivalent encryption.

## 18.10. Testing and Approval Standards

A. No Keno System may be offered for Play unless it has received approval by the Tribal Gaming Agency (TGA) and the State Gaming Agency (SGA). Any modification of a hardware or software component approved under this section must be similarly approved.

B. Any proposal for a system or system component not authorized in these standards shall include a description of the system or component, the proposed manner of regulation, monitoring and/or maintenance of the system, and shall require submission to, and approval by, the TGA and SGA.

C. At the request of TGA or SGA the manufacturer may be required to transport a working model of the Keno System to a location designated by the TGA or SGA for testing, examination or analysis. Neither the SGA nor the TGA shall be liable for any costs associated with the transportation, testing, examination, or analysis, including any damage to the components of the Keno System. If requested by the TGA or SGA, the manufacturer may be required to provide specialized equipment or the services of an independent technical expert to assist with the testing, examination and analysis. For purpose of continued monitoring, the TGA or SGA may retain working models of any Keno System or component after approval for as long as the equipment is in play in the state.

# Chapter 19 SPORTSBOOK

The following definitions apply to this Chapter only.

## 19.1. Definitions

A. Authorized Sports Wagering Menu means the list of leagues, organizations, and types of wagers approved for Sports Wagering.

B. Cloud Storage means data which is stored on remote servers accessed from the internet.

C. Collegiate Sport *or* Athletic Event means a sport or athletic event offered or sponsored by, or played in connection with, a public or private institution that offers education services beyond the secondary level.

D. Electronic Sports *or* Esports Competition *or* Event means a live video game event or tournament attended or watched by members of the public where games or matches are contested in real time by player(s) and team(s), and player(s) or team(s) can win a prize based on their performance in the live video game event or tournament.

E. Geofence means any technology used to create a virtual geographic boundary or technology used to detect the physical location of a device a patron is using to attempt to engage in Mobile Sports Wagering.

F. Integrity Monitoring Provider means a Sports Wagering Vendor approved by the Tribal Gaming Agency and the State Gaming Agency to receive reports of Unusual Wagering Activity from the Gaming Operation for the purpose of assisting in identifying Suspicious Wagering Activity.

G. Layoff Wager means a wager placed or accepted between gaming operations for the purpose of offsetting the tribal Sports Wagering liability.

H. Minor League means a lower professional league or division within a sport, such as American baseball or hockey, where a professional team has the exclusive contractual rights to promote and relegate players.

I. Mobile Device means portable electronic equipment used in Mobile Sports Wagering, including but not limited to a mobile phone, tablet, personal computer, electronic device, and any other portable electronic device.

J. Mobile Sports Wagering means any Sports Wagering on a Mobile Device platform, including Sports Wagers deployed and accessed through the internet or an application installed on a Mobile Device.

K. Player Account means an electronic account established by a patron for the purpose of Sports Wagering, including deposits, withdrawals, wagered amounts, payouts on winning wagers, or similar adjustments.

L. Premises means buildings that comprise a Gaming Facility and adjacent or adjoining amenities, such as hotels, restaurants, conference or entertainment spaces, common areas, parking lots, garages, and other improved areas; provided that such areas constitute Tribal Lands, and provided further, that such areas do not include non-adjoining convenience stores or golf courses.

M. Professional Sport Event *or* Athletic Event means an event that is not a Collegiate Sport Event or Collegiate Athletic Event at which two or more persons participate in a sports or athletic event and receive compensation in excess of actual expenses for their participation in the event. Professional Sport or Athletic Event does not include any Minor League sport.

N. Sports Governing Body means the organization that prescribes final rules and enforces codes of conduct with respect to a sporting event and participants therein.

O. Sports Wager *or* Mobile Sports Wager means the actual bet placed on sporting events, athletic events, or competitions. A sports wager does not include wagers on horse racing authorized pursuant to chapter 67.16 RCW.

P. Sports Wagering means the business of accepting wagers on any of the following sporting events, athletic events, or competitions by any system or method of wagering: (a) a Professional Sport or Athletic Event; (b) a Collegiate Sport or Athletic Event; (c) an Olympic or international sports competition or event; (d) an Electronic Sports or Esports Competition or Event; (e) a combination of sporting events, athletic events, or competitions listed in (a) through (d) of this subsection; or (f) a portion of any sporting event, athletic event, or competition listed in (a) through (d). Sports Wagering does not include the business of accepting wagers on horse racing authorized pursuant to chapter 67.16 RCW.

Q. Sports Wagering Kiosk means an unattended, self-service terminal, machine, or other device provided by the Gaming Operation through which a patron may place or redeem a Sports Wager.

R. Sports Wagering Net Win means the total amount wagered or played less the amounts repaid to winners as reported as gaming revenue on the annual audited financial statements in accordance with Generally Accepted Accounting Principles (GAAP). The amount of wagers placed by the Gaming Operation and amounts received by the Gaming Operation as payments on Layoff Wagers shall not affect the computation of Sports Wagering Net Win.

S. Sports Wagering System means all equipment, hardware, data networks, communications technology, and software used in the operation of Sports Wagering that directly affect the wagering and results of Sports Wagering offered under this Appendix, including the following: (a) Sports Wagering interactive components, including all associated equipment and software that comprise the Sports Wagering platform used in a Sportsbook or used for online or Mobile Sports Wagering; (b) Sports Wagering Kiosks; and (c) ticket or voucher redemption devices. Sports Wagering System does not include a Mobile Device owned and used by a patron to place a Sports Wager.

T. Sports Wagering Vendor means an organization that provides any gaming goods or services in connection with the operation of Sports Wagering.

U. Sportsbook means the Sports Wagering area where transactions are conducted from a counter located in a Sports Wagering lounge or other window locations as approved by the Tribal Gaming Agency, and any window in the cashier's cage designated only for the redemption of winning Sports Wagering tickets.

V. Suspicious Wagering Activity means Unusual Wagering Activity that cannot be explained and is indicative of match fixing, the manipulation of an event, misuse of inside information, or other prohibited activity.

W. Unusual Wagering Activity means abnormal wagering exhibited by a patron or patrons and deemed by the Gaming Operation as a potential indicator of suspicious activity. Abnormal betting activity may include, but is not limited to, the size of a patron's wager, or increased wagering volume on a particular event or wager type.

## 19.2. Sports Wagering Activities & Location TSC: App S, Sec 3

A. The Sportsbook must be located within the Gaming Facility

B. The server or other equipment used to accept and redeem Sports Wagers must be located within the Gaming Facility. Cloud Storage may be used for duplicate or backup Sports Wagering data, provided that such Cloud Storage facilities are located in Washington State.

C. If Mobile Sports Wagering is offered, the Gaming Operation must use a Geofence to ensure that all Mobile Sports Wagering occurs within the Premises.

## 19.3. Sports Wagering Kiosk Locations TSC: App S, Sec 4

A. Sports Wagering Kiosks may be located anywhere within the Premises and are subject to surveillance requirements imposed by Section 19.10

B. Sports Wagering Kiosks located on the gaming floor are subject to the limits on anonymous Sports Wagers described in Section 19.14.A.2

C. Sports Wager Kiosks located off the gaming floor may not allow anonymous Sports Wager or cash redemption.

## 19.4. Standards of Conduct & Operation TSC: App S, Sec 5

A. The Gaming Operation may accept a Sports Wager on any event conducted by a league or organization, provided that the league, organization, and wager type are listed on the Authorized Sports Wagering Menu.

1. A list of Sports Wagers available at the Gaming Operation will be made available to its patrons.
2. The Gaming Operation may apply to the Tribal Gaming Agency in writing to request adding leagues, organizations, or wager types to the Authorized Sports Wagering Menu
    a) The Gaming Operation may not alter the Authorized Sports Wagering Menu without prior regulatory approval.
3. The Gaming Operation must immediately remove any item from the Sports Wagering Menu upon notice from Tribal Gaming Agency that the Sports Wagering Menu contains an offer in violation controls, regulation, or Authorized Sports Wagering Menu.
4. The Gaming Operation must immediately notify the Tribal Gaming Agency if it intends to remove a league, organization, or wager type from its list of available Sports Wagers.
5. The Gaming Operation may make or accept Layoff Wagers, subject to limitations imposed by state and federal laws.
    a) The Gaming Operation must disclose its identity to the entity accepting the Layoff Wager.
    b) Layoff Wagers must be reported to the Tribal Gaming Agency at the time they are made.

## 19.5. Prohibited Activities & Participants TSC: App S, Sec 5.2

A. The Gaming Operation may not accept any Sports Wager on a Minor League sport.

B. Sports Wagers are not transferrable between patrons.

C. No Gaming Employee may advise or encourage patrons to place a Sports Wager of any specific type, kind, subject, or amount. This restriction does not prohibit general advertising, promotional activities, or answering general questions about Sports Wagers.

D. The Gaming Operation will not knowingly accept a Sports Wager on an event where the outcome has already been determined (past posting).

E. The Gaming Operation will make all reasonable efforts to confirm that any patron seeking to engage in Sports Wagering is not a Prohibited Sports Wagering Participant. Prohibited Sports Wagering Participant means:

1. Any individual under 18 years of age;
2. Any individual placing a wager as an agent or proxy;
3. Any athlete whose performance may be used to determine, in whole or in part, the outcome of such wagering;
4. Any person who is an athlete, player, coach, manager, referee or other game official, physician, trainer, team employee or governing body employee, in any sports event overseen by such person's Sports Governing Body;
5. Any person with access to material, exclusive, non-public confidential information about a sports event that is the subject of such wagering;
6. Any person identified to the Tribal Gaming Agency and State Gaming Agency by a Sports Governing Body that the Tribal Gaming Agency and State Gaming Agency agree is a person who should be a Prohibited Sports Wagering Participant;
7. Any person who holds a position of authority or influence sufficient to exert influence over the participants in a sports event that is the subject of a wager;
8. Any person which the Gaming Operation knows or reasonably should know, is placing a wager by, or on behalf of a Prohibited Sports Wagering Participant; and
9. Any person whose participation may undermine the integrity of wagering on a sports event or the conduct of such sports event itself, or any person who is prohibited for other good cause.

## 19.6. Sports Wagering System TSC: App S, Sec 5.3

A. The Sports Wagering System must meet or exceed Gaming Laboratories International's GLI-33: Standards for Event Wagering Systems, and its appendices, as amended or modified. GLI-33, including its appendices and other GLI Standards referenced within the standard, are hereby incorporated into this regulation titled, **Appendix A: GLI Standards for Sportsbook**.

B. Alternative standards may be agreed to by the Tribal Gaming Agency if the standards meet the requirements established in this Regulation.

C. No substantive modification to any Sports Wagering System may be made after testing, certification, and approval of a Sports Wagering System without certification of the modification by an Independent Test Laboratory. The following modifications are not considered substantive and do not require notification:

a) Changes to content not related to any regulated feature;

b) Installation or changes to backup software;

c) Adding or removing users; and

d) Any system configuration changes that have no impact on the accuracy of report information including gaming revenue.

D. The Gaming Operation must perform an annual system integrity and security assessment of the Sports Wagering System. The independent technical expert's report will be submitted to the Tribal Gaming Agency and will include:

1. The scope of review,
2. Name and company affiliation of the individuals who conducted the assessment,
3. Date of assessment,
4. Findings,
5. Recommended corrective action, if applicable, and
6. The Gaming Operation's response to the findings and recommended corrective action, if applicable.

E. The Sports Wagering System must be capable of generating those reports necessary to record the adjusted gross receipts, wagering liability, ticket redemption, and such other information relating to Sports Wagering as deemed necessary by the Tribal Gaming Agency or as required by Internal Controls. These reports may include, but are not limited to:

1. Gaming Operation Revenue reports;
2. Gaming Operation Liability reports;
3. Future Events reports;
4. Significant Events and Alterations reports;
5. Wager Record Information reports;
6. Market Information reports;
7. Contest/Tournament Information reports;
8. Player Account Information reports;
9. Sports Wagering System Information reports;
10. Significant Event Information reports;
11. User Access Information reports; and
12. Any other reports required by the Tribal Gaming Agency.

F. Any technology not specifically authorized by this regulation may be submitted for regulatory approval if the proposed technology will protect, maintain, or enhance current integrity and security standards.

## 19.7. Wagering Limits TSC: App S, Sec 5.4

A. Appropriate Sports Wagering limits will be set by the Gaming Operation, consistent with limitations on anonymous Sports Wagering in accordance with Section 19.14 and the Reserve Requirement in Section 19.8 below.

## 19.8. Reserve Requirements TSC: App S, Sec 5.5

A. The Gaming Operation must have the ability to cover all outstanding Sports Wagering liabilities.

## 19.9. Player Accounts TSC: App S, Sec 5.6

A. A Player Account is required to engage in Mobile Sports Wagering.

1. The Gaming Operation will limit each patron to one active account and username.
2. The Gaming Operation will implement rules and procedures to terminate all accounts of any patron who knowingly and intentionally establishes or seeks to establish multiple active accounts, whether directly or by use of another person as a proxy.

B. To establish a Player Account, a patron must register in-person at the Gaming Facility and provide, at a minimum, the following information:

1. Legal name;
2. Date of birth;
3. Social security number, or the last four digits thereof, or an equivalent identification number for a noncitizen patron, such as a passport or taxpayer identification number;
4. Residential address;
5. Email address, if any; and
6. Telephone number, if any.

C. The Gaming Operation must verify the patron's identity against a form of valid, federal, state, or tribal government-issued photo identification.

D. The Gaming Operation may utilize a third-party know your customer services or governmental database to authenticate a patron's identity or information.

E. Prior to issuing a patron a Player Account, the patron must accept the Gaming Operation's terms and conditions for Sports Wagering, which must, at a minimum, notify the patron that:

1. The Player Account is non-transferable;
2. The patron is prohibited from allowing any other person to access or use the Player Account.

F. A Player Account may be funded with U.S. currency through the use of:

1. Cash;
2. Cash Equivalent;
3. A patron's deposit of cash or vouchers at the Sportsbook or other cashiering location;
4. Promotional credit;
5. Winnings;
6. Adjustments made by the Gaming Operation with documented notification to the patron; or
7. Any other means approved by the Tribal Gaming Agency.

G. The Gaming Operation must implement Player Account controls that meet or exceed those in Gaming Laboratories International's GLI-33: Standards for Event Wagering Systems, as amended or modified, or equivalent standards as approved by the Tribal Gaming Agency (Refer to **Appendix A: GLI Standards for Sportsbook**).

## 19.10. Surveillance TSC: App S, Sec 5.7

A. All physical components of the Sports Wagering System, except wiring, cables, and conduit in which they are located, shall have the ability to be effectively and clandestinely monitored and recorded by means of a Surveillance System in accordance with Tribal Regulation, Compact, and Appendix A.

## 19.11. Accounting Records TSC: App S, Sec 5.8

A. The Gaming Operation must keep detailed, supporting, and subsidiary Sports Wagering records to support those accounting records in accordance with its Internal Controls.

B. The Gaming Operation's Internal Controls must establish minimum audit standards.

## 19.12. Internal Controls TSC: App S, Sec 5.9

A. The Gaming Operation's Internal Controls must include:

1. Description of Gaming Employees who perform essential functions, including

a) Management of Sports Wagering,

b) Supervisory authority over daily operation of Sports Wagering,

c) Overseeing technology issues related to the Sports Wagering System,

d) Acceptance of Sports Wagers in the Sportsbook,

e) Handling payouts on winning tickets/vouchers, and

f) Coordination of compliance efforts related to Sports Wagering;

2. In the event of a failure or malfunction of the Sports Wagering System's ability to pay winning Sports Wagers, the Gaming Operation shall have internal controls detailing the method of paying winning Sports Wagers.

   a) The Gaming Operation shall also file an incident report for each system failure and document the date, time, and reason for the failure along with the date and time the system is restored with the Tribal Gaming Agency;

3. User access controls for Sports Wagering personnel;

4. Segregation of duties;

5. Automated and manual risk management procedures;

6. Procedures for identifying and reporting fraud and suspicious conduct, including identifying Unusual Wagering Activity and Suspicious Wagering Activity and reporting such activity to an Integrity Monitoring Provider;

7. Procedures for identifying and preventing Sports Wagering by Prohibited Sports Wagering Participants;

8. Description of anti-money laundering compliance standards, which must include limitations placed on anonymous wagering and prohibit anonymous single Sports Wagers of $2,000 or more, and include the retention of the wager record information with patron identification;

9. Process for submitting or receiving approval of all types of wagers available to be offered by the Sports Wagering System;

10. Description of process for accepting Sports Wagers and issuing pay outs, plus any additional controls for accepting Sports Wagers and issuing pay outs in excess of $10,000;

11. Description of a process for accepting multiple Sports Wagers from one patron in a 24-hour cycle, including a process to identify patron structuring of Sports Wagers to circumvent recording and reporting requirements;

12. Opening and closing Sportsbook windows;

13. Procedures for reconciliation of assets and documents contained in a Sports Wagering area cashier's drawer, Sports Wagering Kiosk, and Mobile Sports Wagering, which must include the drop and count

procedures for Sports Wagering Kiosks;

14. Procedures for cashing winning tickets at the cage after the Sportsbook has closed, if applicable;
15. Procedures for accepting value game chips for Sports Wagering, if applicable;
16. Procedures for issuance and acceptance of promotion funds and free wagers for Sports Wagering, if applicable;
17. Description of all integrated third-party systems;
18. If Cloud Storage is utilized, a description of how the Cloud Storage complies with applicable federal laws and a description of how the Cloud Storage meets or exceeds the security standards from Center for Internet Security (CIS), as amended or modified, or equivalent standards as approved by the Tribal Gaming Agency with concurrence from State Gaming Agency.
19. Procedures for closing out dormant Player Accounts;
20. Procedures for making adjustments to a Player Account, including the process for a patron to close out a Player Account, and a process whereby a patron will be refunded after the closure of a Player Account;
21. If the Sports Wagering System includes Mobile Sports Wagering, a method for verifying patrons' wagers placed within the Premises;
22. Procedures to maintain the security of identity and financial information of patrons;
23. Procedures for securely issuing, modifying, and resetting a Player Account password, personal identification number, biometric login, or other approved security feature, when applicable;
24. Procedures for patron notification including any password or security modification via electronic or regular mail, text message, or other manner approved by the Tribal Gaming Agency, provided that such methods will include, at a minimum: (A) if in person, verify the patron's identity against a form of valid, federal, state, or tribal government-issued, photo identification, (B) the correct response to two or more challenge questions, (C) strong authentication, or (D) two-factor authentication;
25. Controls to prevent ACH fraud regarding failed ACH deposits into a Player Account and policies regarding Player Account closure, dormant Player Account, unclaimed funds in a dormant Player Account, and suspension and subsequent restoration of a Player Account;
26. Change control procedure;
27. Procedures for receiving, investigating and responding to patron complaints;

28. Procedures to ensure security of the Sports Wagering System and its components, both physical and logical, continuously throughout system's or system component's lifecycle;
29. Procedures for line setting and line moving;
30. Procedures regarding redemption of winning tickets, including but not limited to a method for redeeming lost tickets, if allowed, and a method for redeeming tickets by U.S. Mail, if allowed;
31. Description of the circumstances, limitations, and method by which the Gaming Operation will cancel wagers, which must at a minimum require cancellation in the event of an obvious error and require that only a supervisory employee of the Gaming Operation can void or cancel a wager;
32. Procedures for voiding wagers;
33. Accounting and audit procedures; and
34. Any other internal controls deemed necessary by the State Gaming Agency and Tribal Gaming Agency by memorandum of agreement.

B. Any new or revised Internal Controls proposed by the Gaming Operation shall:
1. Ensure that the interests of the Tribe relating to Sports Wagering are preserved and protected;
2. maintain the integrity of Sports Wagering; and
3. Reduce the dangers of unfair or illegal practices in the conduct of Sports Wagering.

## 19.13. House Rules TSC: App S, Sec 5.10

A. The Gaming Operation will adopt comprehensive house rules, which must be approved by the Tribal Gaming Agency, and made available to patrons at the Gaming Facility and through the Sports Wagering System.

B. House Rules shall include:
1. Method for calculation and payment of winning wagers;
2. Description of the process for handling incorrectly posted events, odds, wagers, or results;
3. Effect of schedule changes;
4. Method of notifying patrons of odds or proposition changes;
5. Acceptance of wagers at other than posted terms;
6. Expiration of any winning ticket;
7. Lost ticket policy;
8. Method of contacting the operator for questions and complaints;

9. A policy by which Gaming Operation can cancel or void wagers; and
10. Description of Prohibited Sports Wagering Participants.

## 19.14. Anti-Money Laundering TSC: App S, Sec 7.1

A. The Gaming Operation must adhere to the following limits on Anonymous Wagering:
   1. No patron shall engage in Mobile Sports Wagering, as provided in Section 19.9 of this Appendix, without a Player Account.
   2. No patron may anonymously place a single Sports Wager of $2,000 or more. The Internal Controls will detail acceptable forms and methods of identifying a patron who places a wager of $2,000 or more.

## 19.15. Sports Integrity TSC: App S, Sec 7.2

A. To ensure the Tribal Gaming Agency can monitor the integrity of Sports Wagering, the Gaming Operation will require the collection of aggregate Sports Wagering information, in a format that can be efficiently utilized, provided to, and analyzed by an approved Integrity Monitoring Provider.

B. In order to identify Unusual Wagering Activity and Suspicious Wagering Activity, the Integrity Monitoring Provider will monitor Sports Wagering information as outlined in the Internal Controls that includes industry best practices.

C. Upon receiving any report of Unusual Wagering Activity or Suspicious Wagering Activity from an Integrity Monitoring Provider, the Gaming Operation will review such reports and notify the Integrity Monitoring Provider of whether or not it has experienced similar activity.

D. As a condition of licensure by the Tribal Gaming Agency, the Integrity Monitoring Provider will be required to:
   1. Share information about any Unusual Wagering Activity with other Integrity Monitoring Providers and required to disseminate all reports of Unusual Wagering Activity to all tribes offering Sports Wagering in Washington; and
   2. Immediately notify all other Integrity Monitoring Providers, the Tribal Gaming Agency, and the State Gaming Agency if the Integrity Monitoring Provider finds any Suspicious Wagering Activity, including a previously reported Unusual Wagering Activity that rises to the level of Suspicious Wagering Activity.

## 19.16. Problem & Responsible Gambling TSC: App S, Sec 8.2

A. Each Mobile Sports Wagering application and each Sports Wagering Kiosk shall display a commitment to responsible gambling and a link to the policy created pursuant to Compact Appendix E, Section 8.2.

B. Either through the Mobile Sports Wagering application or through the Player Accounts, the Tribe shall include the option to self-impose limitations on wagering parameters including, at a minimum,

1. Limits on the dollar amount of deposits a player can make into his or her Player Account within a specified time period, and
2. Limits on the total amount of time available for play or wagering during a specified time period.

# Chapter 20 PATRON DEPOSIT ACCOUNTS & CASHLESS SYSTEMS

## 20.1. Supervision.

A. Supervision must be provided as needed for patron deposit accounts and cashless systems by an agent(s) with authority equal to or greater than those being supervised.

## 20.2. Patron deposit accounts and cashless systems.

A. Smart cards cannot maintain the only source of account data.

B. Establishment of patron deposit accounts. The following standards apply when a patron establishes an account.

1. The patron must appear at the gaming operation in person, at a designated area of accountability, and present valid government issued picture identification; and
2. An agent must examine the patron's identification and record the following information:
    a) Type, number, and expiration date of the identification;
    b) Patron's name;
    c) A unique account identifier;
    d) Date the account was opened; and
    e) The agent's name.
3. The patron must sign the account documentation before the agent may activate the account.
4. The agent or cashless system must provide the patron deposit account holder with a secure method of access.

C. Patron deposits, withdrawals and adjustments.

1. Prior to the patron making a deposit or withdrawal from a patron deposit account, the agent or cashless system must verify the patron deposit account, the patron identity, and availability of funds. A personal identification number (PIN) is an acceptable form of verifying identification.
2. Adjustments made to the patron deposit accounts must be performed by an agent.
3. When a deposit, withdrawal, or adjustment is processed by an agent, a transaction record must be created containing the following information:

a) Same document number on all copies;

b) Type of transaction, (deposit, withdrawal, or adjustment);

c) Name or other identifier of the patron;

d) The unique account identifier;

e) Patron signature for withdrawals, unless a secured method of access is utilized;

f) For adjustments to the account, the reason for the adjustment;

g) Date and time of transaction;

h) Amount of transaction;

i) Nature of deposit, withdrawal, or adjustment (cash, check, chips); and

j) Signature of the agent processing the transaction.

4. When a patron deposits or withdraws funds from a patron deposit account electronically, the following must be recorded:

a) Date and time of transaction;

b) Location (player interface, kiosk);

c) Type of transaction (deposit, withdrawal);

d) Amount of transaction; and

e) The unique account identifier.

5. Patron deposit account transaction records must be available to the patron upon reasonable request.

6. If electronic funds transfers are made to or from a gaming operation bank account for patron deposit account funds, the bank account must be dedicated and may not be used for any other types of transactions.

D. Variances. The operation must establish, as approved by the TGRA, the threshold level at which a variance must be reviewed to determine the cause. Any such review must be documented.

# Chapter 21 LINES OF CREDIT

## 21.1. Supervision.

A. Supervision must be provided as needed for lines of credit by an agent(s) with authority equal to or greater than those being supervised.

## 21.2. Establishment of lines of credit policy.

A. If a gaming operation extends lines of credit, controls must be established and procedures implemented to safeguard the assets of the gaming operation. Such controls must include a lines of credit policy including the following:

1. A process for the patron to apply for, modify, and/or re-establish lines of credit, to include required documentation and credit line limit;
2. Authorization levels of credit issuer(s);
3. Identification of agents authorized to issue lines of credit;
4. A process for verifying an applicant's credit worthiness;
5. A system for recording patron information, to include:
    a) Name, current address, and signature;
    b) Identification credential;
    c) Authorized credit line limit;
    d) Documented approval by an agent authorized to approve credit line limits;
    e) Date, time and amount of credit issuances and payments; and
    f) Amount of available credit.
6. A process for issuing lines of credit to:
    a) Verify the patron's identity;
    b) Notify the patron of the lines of credit terms, including obtaining patron's written acknowledgment of the terms by signature;
    c) Complete a uniquely identified, multi-part, lines of credit issuance form, such as a marker or counter check, which includes the terms of the lines of credit transaction;
    d) Obtain required signatures;
    e) Determine the amount of the patron's available lines of credit;
    f) Update the credit balance record at the time of each transaction to ensure that lines of credit issued are within the established limit and balance for that patron; and
    g) Require the agent issuing the lines of credit to be independent of the agent who authorized the lines of credit.

7. A policy establishing credit line limit exceptions to include the following:
    a) Identification of the agent(s) authorized to permit a credit line limit to be exceeded;
    b) Authorization thresholds; and
    c) Required documentation.
8. A policy governing increases and decreases to a patron's lines of credit account balances to include the following:
    a) Documentation and record keeping requirements;
    b) Independence between the department that receives the payment and the department that maintains custody of the credit balance for payments made by mail;
    c) Collections;
    d) Periodic audits and confirmation of balances; and
    e) If a collection agency is used, a process to ensure documentation of increases and decreases to the lines of credit account balances.
9. A policy governing write-offs and settlements to include:
    a) Identification of agent(s) authorized to approve write-offs and settlements;
    b) Authorization levels for write-offs and settlements of lines of credit instruments;
    c) Required documentation for write-offs and settlements;
    d) Independence between the agent who established the lines of credit and the agent writing off or settling the lines of credit instrument; and
    e) Necessary documentation for the approval of write-offs and settlements and transmittal to the appropriate department for recording and deductibility.

## 21.3. Variances.

A. The operation must establish, as approved by the TGRA, the threshold level at which a variance must be reviewed to determine the cause. Any such review must be documented.

# Chapter 22 ELECTRONIC TABLE GAMES

The following terms apply to this chapter only.

## 22.1. Definitions TSC, Appendix G, Section 2

A. Component means Electronic Table Game Terminals, any dealer interface, the Electronic Wagering System, and hardware, software, and servers that function collectively to simulate table game operations and are necessary to operate the Electronic Table Game System.

B. Communal Shoe means a randomly shuffled and dealt deck or decks of cards, whether physical or electronic, that removes each card played until the round of play is completed according to the approved game rules.

C. Electronic Table Game *or* ETG means an electronic version of a Class III table game.

D. Electronic Table Game System *or* ETG System means a system that utilizes electronics in connection with the generation, collection, storage, and communication of game outcome, accounting, and significant event data, including all Components thereof, to operate Electronic Table Games.

E. Electronic Table Game Terminal *or* ETG Terminal means a computer housed in a cabinet with input device(s) and video screen(s) where a player may play Electronic Table Games.

F. Electronic Wagering System means a Component of the ETG System that includes a computer or server and any related hardware, software or other device that facilitates patron play at an Electronic Table Game.

## 22.2. Authorization, Conditions, and Limitations TSC, Appendix G, Section 3

A. ETG Systems must be secure, reliable, auditable, and compliant with the standards contained in this regulation.

B. ETG Systems that do not allow patrons to Play Against the Machine are authorized. An ETG System does not allow Play Against the Machine when:

1. There is a human dealer involved in the play of the ETG (Dealer Controlled); or
2. The play of the ETG does not involve a human dealer, and the ETG System is configured for play between two or more patrons against the same roll of dice or spin of the wheel, or a Communal Shoe of electronic cards (Non-Dealer Controlled); however only one patron is needed to initiate game play; or
3. It is a hybrid of Dealer Controlled and Non-Dealer Controlled, provided that any ETG played as Dealer Controlled follows applicable Dealer-Controlled standards set forth in this regulation and any ETG offered as

Non-Dealer Controlled follows applicable Non-Dealer Controlled standards set forth in this regulation.

C. Games

1. An ETG version of any currently approved Class III Table Game may be offered for play.

   a) Pay table or odds offered on an ETG shall be consistent with approved game rules.

   b) ETG game rules must be displayed on each ETG Terminal.

2. An ETG Terminal may allow for play any other Class III activity as authorized under the Compact and Appendices, other than the Tribal Lottery System or any Gaming activity with a limited allocation.

3. Concurrent play. Patrons may play more than one ETG concurrently using a single ETG Terminal under the following requirements:

   a) An ETG Terminal must display clear information about each ETG available for play and such information must be available to a patron without the patron first placing a wager.

   b) An ETG Terminal must display each ETG selected for play by the patron.

   c) An ETG Terminal must display the decisions and outcomes of play for each ETG selected by the patron.

   d) An ETG may not be added to or removed from an ETG Terminal in use by a patron.

D. Wager limits for ETGs shall not exceed $500.

E. An ETG shall be activated with an Electronic Wagering System that meets the standards described in Section 22.3.A.2.

F. An ETG Terminal shall not issue coin or U.S. currency at the conclusion of a patron's play.

G. Every nine (9) ETG Terminals shall constitute one Gaming Station. If the number of ETG Terminals put into play is not perfectly divisible by nine (9), then any remainder less than nine (9) will constitute a Gaming Station. For example, if ten (10) ETG Terminals are in operation, it will constitute two (2) Gaming Stations. (TSC, Appendix G, Section 4)

## 22.3. Operation & Reporting Requirements TSC, Appendix G, Section 5

A. Any ETG must comply with the standards established by this regulation and any applicable provision of the Compact and must meet or exceed all applicable standards of Gaming Laboratories International's Standards GLI-24: Electronic Table Game Systems and GLI-25: Dealer Controlled Electronic Table Games, as amended or modified. GLI-24 and GLI-25 Standards are hereby incorporated into

this regulation titled, **Appendix B: GLI Standards for Electronic Table Games**.

1. Any standards that contemplate features or functionalities of an ETG System that conflict with Section 22.2 of this chapter are not applicable, and such features or functionalities are prohibited.
2. Any Electronic Wagering System must meet or exceed Gaming Laboratories International's Standard GLI-16: Cashless Systems in Casinos, the standards established by this chapter, any applicable provision of the Compact, including Cashless Transaction System as defined in Appendix X2, and any related MOU. GLI-16 Standards are hereby incorporated into this regulation titled, **Appendix B: GLI Standards for Electronic Table Games**.
    a) Any "Cashless Systems in Casinos" that would add money to or take money from a patron's account without a cashier or kiosk are prohibited until negotiated and agreed upon by the Tribe and State.
3. The Gaming Operation may propose alternative standards for any ETG System authorized in Section 22.2, in lieu of standards contained in **Appendix B: GLI Standards for Electronic Table Games**.
    a) Any proposed alternative standards must maintain the integrity and security of the ETG System.
    b) Proposed alternative standards must be drafted and submitted to the Tribal Gaming Agency for consideration.

B. Internal Controls are required to include, at a minimum:

1. Description of Gaming Employees who perform essential functions, supervisory authority, handling payouts on winning vouchers.
2. User access controls for ETG personnel;
3. Segregation of duties;
4. Procedures for receiving, investigation and responding to patron complaints;
5. Accounting and audit procedures;
6. Procedures to ensure the physical security of the ETG Systems, including key controls and Closed Surveillance System coverage;
7. Procedures to ensure the integrity and security of all sensitive data and software;
8. Procedures to ensure that access to sensitive data and software is limited to appropriate personnel;
9. Procedures to ensure accurate accounting of wagers and payouts;
10. Procedures to ensure the logging of the events and the availability of records to permit an effective it of the conduct of the ETG System and

the reporting of revenue;

11. Policies and Procedures for complying with applicable federal Anti-Money Laundering requirements. (TSC, Appendix G, Section 9)
12. All existing Internal Controls are updated, as necessary, to ensure there are no conflicts with any Internal Controls governing ETG Systems;
13. Procedures for Opening and Closing an ETG(s) when using a live dealer; and
14. Any other internal controls deemed necessary by the State Gaming Agency and Tribal Gaming Agency.

C. The ETG System must be capable of recording information and generating reports as deemed necessary by the Tribal Gaming Agency or as required by Internal Controls. These reports may include, but are not limited to, all applicable reports as outlined in **Appendix B: GLI Standards for Electronic Table Games,** GLI-24, Section 2.21.

D. A manufacturer's prototype (e.g., test cart) of the version of the ETG System that will be installed at the Gaming Facility will be delivered to the State Gaming Agency for training purposes prior to field testing.

## 22.4. Approval of Electronic Table Game Systems TSC, Appendix G, Section 6

A. The general purpose of testing an ETG System pursuant to this Section is to determine the compliance of the ETG System with this regulation and its appendices.

B. Each new or upgraded ETG System may be offered for play only if it has been tested and certified as meeting the applicable standards of this regulation by an Independent Test Laboratory (ITL).

C. At the conclusion of testing, the ITL shall provide to the Tribal Gaming Agency its certification and supporting documentation. If the ITL provides sufficient documentation that the ETG System or relevant Component has been tested and certified by that ITL in any other jurisdiction and it meets the requirements of this regulation, without any subsequent modifications, that shall be sufficient to satisfy this requirement.

D. No substantive modification to any ETG System may be made after testing, certification, and approval without certification of the modification by an ITL. The following modifications are not considered substantive and do not require ITL certification:

1. Changes to content not related to any regulated feature;
2. Adding or removing users;
3. Any system configuration changes that have no impact on the accuracy of report information including gaming revenue; and

4. Minor modifications to hardware.

## 22.5. Field Testing for ETG Systems TSC, Appendix G, Section 6.3

A. A new ETG System may only be offered for play subject to field testing at the Tribe's Gaming Facility in accordance with Field Testing Requirements established by the Tribal Gaming Agency.

B. The Gaming Operation is not required to complete Field Testing if the same ETG System using the same configuration has been successfully completed and approved by another tribe.

## 22.6. Problem & Responsible Gambling TSC, Appendix G, Section 8.2

A. Each ETG Terminal is required to display a responsible gambling message and a link to the Gaming Operation's responsible gambling policy.

# *Appendix A: GLI Standards for Sportsbook*

# GLI STANDARD SERIES

# GLI-33:

# STANDARDS FOR EVENT WAGERING SYSTEMS

**VERSION: 1.1**

**REVISION DATE: MAY 14, 2019**

# About This Standard

**Gaming Laboratories International, LLC (GLI)** has developed this technical standard for the purpose of providing independent technical analysis and/or certifications to gaming industry stakeholders indicating the state of compliance for gaming operations and systems with the requirements set forth herein.

Operators and suppliers are expected to provide documentation, credentials, and associated access to a production equivalent test environment with a request to the independent testing laboratory that it be evaluated in accordance with this technical standard. Upon the successful completion of testing, the independent testing laboratory will provide a certificate of compliance evidencing the certification to this standard.

GLI-33 should be viewed as a living document that will be tailored periodically to align with this developing industry over time as gaming implementations and operations evolve.

# Table of Contents

# Chapter 1: Introduction to Event Wagering Systems

## 1.1 Introduction

### 1.1.1 General Statement

**Gaming Laboratories International, LLC (GLI)** has been testing gaming equipment since 1989. Over the years, GLI has developed numerous technical standards utilized by jurisdictions all over the world. This document, *GLI-33*, sets forth the technical standards for Event Wagering Systems.

### 1.1.2 Document History

This document is a compilation based upon many standards documents from around the world. Some were written by GLI; others were written by industry regulators with input from independent test laboratories and Event Wagering System operators, developers, and suppliers. GLI has taken each of the standards documents and merged the unique rules, eliminated some rules and updated others, to reflect both the change in technology and the purpose of maintaining an objective standard that achieves common regulatory objectives without unnecessarily impeding technological innovation. GLI lists below, and gives credit to, agencies whose documents were reviewed prior to writing this Standard. It is the policy of GLI to update this document as often as warranted to reflect changes in technology and/or testing methods. This document will be distributed without charge and may be obtained by downloading it from the GLI website at www.gaminglabs.com or by contacting GLI at:

**Gaming Laboratories International, LLC.**
600 Airport Road
Lakewood, NJ 08701
Phone: (732) 942-3999
Fax: (732) 942-0043

## 1.2 Acknowledgment of Other Standards Reviewed

### 1.2.1 General Statement

This technical standard has been developed by reviewing and using portions of documents from the following organizations. GLI acknowledges and thanks the regulators and other industry participants who have assembled these documents:

a) Nevada Gaming Commission and Gaming Control Board.
b) British Columbia Gaming Policy and Enforcement Branch (GPEB).
c) Association of Racing Commissioners International (ARCI).
d) Tasmanian Liquor and Gaming Commission.
e) Northern Territory Racing Commission.
f) Victorian Commission for Gambling and Liquor Regulation.
g) Danish Gambling Authority.
h) Spanish Directorate General for the Regulation of Gambling (DGOJ).

i) South African Bureau of Standards (SABS).

## 1.3 Purpose of Technical Standards

### 1.3.1 General Statement

The purpose of this technical standard is as follows:

a) To eliminate subjective criteria in analyzing and certifying Event Wagering Systems.
b) To test the criteria that impact the credibility and integrity of Event Wagering Systems from both the revenue collection and player's perspective.
c) To create a standard that will ensure wagers on events are fair, secure, and able to be audited and operated correctly.
d) To distinguish between local public policy and Independent Test Laboratory criteria. It is up to each local jurisdiction to set its own public policy with respect to wagering.
e) To recognize that the evaluation of internal control systems (such as Anti-Money Laundering, Financial and Business processes) employed by the operators of the Event Wagering System should not be incorporated into the laboratory testing of the standard but instead be included within the operational audit performed for local jurisdictions.
f) To construct a standard that can be easily revised to allow for new technology.
g) To construct a standard that does not specify any particular design, method, or algorithm. The intent is to allow a wide range of methods to be used to conform to the standards, while at the same time encourage new methods to be developed.

### 1.3.2 No Limitation of Technology

One should be cautioned that this document shall not be read in such a way that limits the use of future technology. This document should not be interpreted to mean that if the technology is not mentioned, then it is not allowed. To the contrary, GLI will review this standard and make changes to incorporate minimum standards for any new and related technology.

### 1.3.3 Adoption and Observance

This technical standard can be adopted in whole or in part by any regulatory body that wishes to implement a comprehensive set of requirements for Event Wagering Systems.

## 1.4 Other Documents That May Apply

### 1.4.1 Other GLI Standards

This technical standard covers the requirements for Event Wagering Systems. Depending on the technology utilized by a system, additional GLI technical standards may also apply.

**NOTE:** The entire family of GLI Standards is available free of charge at www.gaminglabs.com.

### 1.4.2 Operator's Minimum Internal Control Standards (MICS)

The implementation of an Event Wagering System is a complex task, and as such will require the development of internal processes and procedures to ensure that the system is configured and operated with the necessary level of security and control. To that end, it is expected that the operator will establish a set of Minimum Internal Control Standards (MICS) to define the internal processes for the creation, management, and handling of wagering transactions as well as the requirements for internal control of any system or component software and hardware, and their associated accounts.

## 1.5 Interpretation of this Document

### 1.5.1 General Statement

This technical standard applies to systems that support wagering on sports, competitions, matches, and other event types approved by the regulatory body. The requirements in this technical standard apply to wagering on events in a way that is general in nature and does not limit or authorize specific events, markets or types of wagers. The intent is to provide a framework to cover those currently known and permitted by law. This document is not intended to define which parties are responsible for meeting the requirements of this technical standard. It is the responsibility of the stakeholders of each operator to determine how to best meet the requirements laid out in this document.

### 1.5.2 Software Suppliers and Operators

The components of an Event Wagering System, although they may be constructed in a modular fashion, are designed to work seamlessly together. In addition, Event Wagering Systems may be developed to have configurable features; the final configuration of which depends on the options chosen by the operator. From a testing perspective, it might not be possible to test all of the configurable features of an Event Wagering System submitted by a software supplier in the absence of the final configuration chosen by the operator; however, the configuration that will be utilized in the production environment shall be communicated to the independent test laboratory to facilitate creating a functionally equivalent test environment. Because of the integrated nature of an Event Wagering System, there are several requirements in this document which may apply to both operators and suppliers. In these cases, where testing is requested for a "white-label" version of the system, a specific configuration will be tested and reported.

## 1.6 Testing and Auditing

### 1.6.1 Laboratory Testing

The independent test laboratory will test and certify the components of the Event Wagering System in accordance with the chapters of this technical standard within a controlled test environment, as applicable. Any of these requirements which necessitate additional operational procedures to meet the intent of the requirement shall be documented within the evaluation report and used to supplement the scope of the operational audit.

### 1.6.2 Operational Audit

The integrity and accuracy of the operation of an Event Wagering System is highly dependent upon operational procedures, configurations, and the production environment's network infrastructure. As such, an operational audit is an essential addition to the testing and certification of an Event Wagering System. The operational audit, outlined within the following appendices of this technical standard, shall be performed at a frequency specified by the regulatory body:

a) Appendix A: Operational Audit of Wagering Procedures and Practices. This includes, but is not limited to, review of the MICS, procedures and practices for wagering operations, including, but not limited to establishing wagering rules, suspending events, handling various wagering and financial transactions, creating markets, settling wagers, closing markets, cancellations of events, voiding or cancelling wagers, player account management, fundamental practices relevant to the limitation of risks, and any other objectives established by the regulatory body.
b) Appendix B: Operational Audit of Technical Security Controls. This includes, but is not limited to, an information security system (ISS) assessment, review of the operational processes that are critical to compliance, penetration testing focused on the external and internal infrastructure as well as the applications transferring, storing and/or processing of player data and/or sensitive information, and any other objectives established by the regulatory body.

# Chapter 2: System Requirements

## 2.1 Introduction

### 2.1.1 General Statement

If the Event Wagering System is comprised of multiple computer systems at various sites, the system as a whole and all communication between its components shall conform to the applicable technical requirements within this document.

## 2.2 System Clock Requirements

### 2.2.1 System Clock

The Event Wagering System shall maintain an internal clock that reflects the current date and time that shall be used to provide for the following:

a) Time stamping of all transactions and events;
b) Time stamping of significant events; and
c) Reference clock for reporting.

### 2.2.2 Time Synchronization

The Event Wagering System shall be equipped with a mechanism to ensure the time and dates between all components that comprise the system are synchronized.

## 2.3 Control Program Requirements

### 2.3.1 General Statement

In addition to the requirements contained within this section, the auditing procedures indicated in the "Verification Procedures" section of this document shall also be met.

### 2.3.2 Control Program Self-Verification

The Event Wagering System shall be capable of verifying that all critical control program components contained on the system are authentic copies of the approved components of the system, upon installation, at least once every 24 hours, and on demand using a method approved by the regulatory body. The critical control program authentication mechanism shall:

a) Employ a hash algorithm which produces a message digest of at least 128 bits;
b) Include all critical control program components which may affect wagering operations, including but not limited to: executables, libraries, wagering or system configurations, operating system files, components that control required system reporting, and database elements that affect system operations; and

c) Provide an indication of the authentication failure if any critical control program component is determined to be invalid.

### 2.3.3 Control Program Independent Verification

Each critical control program component of the Event Wagering System shall have a method to be verified via an independent third-party verification procedure. The third-party verification process shall operate independently of any process or security software within the system. The independent test laboratory, prior to system approval, shall approve the integrity check method.

### 2.3.4 Shutdown and Recovery

The Event Wagering System shall be able to perform a graceful shut down, and only allow automatic restart on power up after the following procedures have been performed at a minimum:

a) Program resumption routine(s), including self-tests, complete successfully;
b) All critical control program components of the system have been authenticated using a method approved by the regulatory body; and
c) Communication with all components necessary for system operation have been established and similarly authenticated.

## 2.4 Wagering Management

### 2.4.1 Wagering Management

The Event Wagering System shall be able to suspend the following on demand:

a) All wagering activity;
b) Individual events;
c) Individual markets;
d) Individual Wagering Devices (if applicable); and
e) Individual player logins (if applicable).

## 2.5 Player Account Management

### 2.5.1 General Statement

The requirements of this section apply to player accounts where supported by the Event Wagering System. In addition to the requirements contained within this section, the "Player Account Controls" section of this document shall also be met.

**NOTE:** Player account registration and verification are required by the Event Wagering System for a player to participate in remote wagering.

### 2.5.2 Registration and Verification

There shall be a method to collect player information prior to the registration of a player account. Where player account registration and verification are supported by the Event Wagering System either directly by the system or in conjunction with a third-party service provider's software, the following requirements shall be met:

a) Only players of the legal wagering age for the jurisdiction may register for a player account. Any person that submits a birth date that indicates they are underage shall be denied the ability to register for a player account.
b) Identity verification shall be undertaken before a player is allowed to place a wager. Third-party service providers may be used for identity verification as allowed by the regulatory body.
    i. Identity verification shall authenticate the legal name, physical address and age of the individual at a minimum as required by the regulatory body.
    ii. Identity verification shall also confirm that the player is not on any exclusion lists held by the operator or the regulatory body or prohibited from establishing or maintaining an account for any other reason.
    iii. Details of identity verification shall be kept in a secure manner.
c) The player account can only become active once age and identity verification are successfully completed, the player is determined to not be on any exclusion lists or prohibited from establishing or maintaining an account for any other reason, the player has acknowledged the necessary privacy policies and terms and conditions, and the player account registration is complete.
d) A player shall only be permitted to have one active player account at a time unless specifically authorized by the regulatory body.
e) The system shall allow the ability to update passwords, registration information and the account used for financial transactions for each player. A multi-factor authentication process shall be employed for these purposes.

### 2.5.3 Player Access

A player accesses their player account using a username (or similar) and a password or a secure alternative means for the player to perform authentication to log in to the Event Wagering System. Authentication methods are subject to the discretion of the regulatory body as necessary. The requirement does not prohibit the option for more than one method of authentication being available for a player to access their account.

a) If the system does not recognize the username and/or password when entered, an explanatory message shall be displayed to the player which prompts the player to re-enter the information.
b) Where a player has forgotten their username and/or password, a multi-factor authentication process shall be employed for the retrieval of the username/resetting of the password.
c) Current account balance information and transaction options shall be available to the player once authenticated.
d) The system shall support a mechanism that allows for an account to be locked in the event that suspicious activity is detected (e.g., too many failed attempts for login). A multi-factor authentication process shall be employed for the account to be unlocked.

### 2.5.4 Player Inactivity

For player accounts accessed remotely for wagering or account management, after 30 minutes of inactivity on that device, or a period determined by the regulatory body, the player shall be required to re-authenticate to access their player account.

a) No further wagering or financial transactions on that device are permitted until the player has been re-authenticated.
b) A simpler means may be offered for a player to re-authenticate on that device, such as operating system-level authentication (e.g., biometrics) or a Personal Identification Number (PIN). Each means for re-authentication will be evaluated on a case-by-case basis by the independent test laboratory.
    i. This functionality may be disabled based on preference of the player and/or regulatory body.
    ii. Once every 30 days, or a period specified by the regulatory body, the player will be required to provide full authentication on that device.

### 2.5.5 Limitations and Exclusions

The Event Wagering System shall be able to correctly implement any limitations and/or exclusions put in place by the player and/or operator as required by the regulatory body:

a) Where the system provides the ability to directly manage limitations and/or exclusions, the applicable requirements within the "Limitations" and "Exclusions" sections of this document shall be evaluated;
b) The self-imposed limitations set by a player shall not override more restrictive operator-imposed limitations. The more restrictive limitations shall take priority; and
c) Limitations shall not be compromised by internal status events, such as self-imposed exclusion orders and revocations.

### 2.5.6 Player Funds Maintenance

Where financial transactions can be performed automatically by the Event Wagering System the following requirements shall be met:

a) The system shall provide confirmation/denial of every financial transaction initiated.
b) A deposit into a player account may be made via a credit card transaction or other methods which can produce a sufficient audit trail.
c) Funds shall not be available for wagering until they are received from the issuer or the issuer provides an authorization number indicating that the funds are authorized. The authorization number is to be maintained in an audit log.
d) Payments from an account are to be paid (including funds transfer) directly to an account with a financial institution in the name of the player or made payable to the player and forwarded to the player's address using a secure delivery service or through another method that is not prohibited by the regulatory body. The name and address are to be the same as held in player registration details.
e) If a player initiates a player account transaction and that transaction would exceed limits put in

place by the operator and/or regulatory body, this transaction may only be processed provided that the player is clearly notified that they have withdrawn or deposited less than requested.

f) It shall not be possible to transfer funds between two player accounts.

### 2.5.7 Transaction Log or Account Statement

The Event Wagering System shall be able to provide a transaction log or account statement history to a player upon request. The information provided shall include sufficient information to allow the player to reconcile the statement or log against their own financial records. Information to be provided shall include at a minimum, details on the following types of transactions:

a) Financial Transactions (time stamped with a unique transaction ID):
   i. Deposits to the player account;
   ii. Withdrawals from the player account;
   iii. Promotional or bonus credits added to/removed from the player account (outside of credits won in wagering);
   iv. Manual adjustments or modifications to the player account (e.g., due to refunds);
b) Wagering Transactions:
   i. Unique identification number of the wager;
   ii. The date and time the wager was placed;
   iii. The date and time the event started and ended or is expected to occur for future events (if known);
   iv. The date and time the results were confirmed (blank until confirmed);
   v. Any player choices involved in the wager, including market and line postings, wager selection, and any special condition(s) applying to the wager;
   vi. The results of the wager (blank until confirmed);
   vii. Total amount wagered, including any promotional/bonus credits (if applicable);
   viii. Total amount won, including any promotional/bonus credits (if applicable);
   ix. Commission or fees collected (if applicable); and
   x. The date and time the winning wager was paid to the player.

### 2.5.8 Player Loyalty Programs

Player loyalty programs are any programs that provide incentives for players, typically based on the volume of play or revenue received from a player. If player loyalty programs are supported by the Event Wagering System, the following principles shall apply:

a) All awards shall be equally available to all players who achieve the defined level of qualification for player loyalty points;
b) Redemption of player loyalty points earned shall be a secure transaction that automatically debits the points balance for the value of the prize redeemed; and
c) All player loyalty points transactions shall be recorded by the system.

## 2.6 Wagering Instrument Functionality

### 2.6.1 General Statement

Event Wagering Systems which support the issuance and/or redemption of wagering instruments (vouchers and coupons) shall meet the applicable requirements established within the "Machine Vouchers" section of the *GLI-11 Standards for Gaming Devices* and the "Validation System Requirements" of the *GLI-13 Standards for On-Line Monitoring and Control Systems (MCS) and Validation Systems* and other applicable jurisdictional requirements observed by the regulatory body.

## 2.7 Location Requirements for Remote Wagering

### 2.7.1 General Statement

Where required by the regulatory body, the requirements within this section shall apply when the Event Wagering System supports remote wagering.

**NOTE:** The operator or third-party service provider maintaining these components, services and/or applications shall meet the auditing procedures indicated in the "Location Service Provider" section of this document.

### 2.7.2 Location Fraud Prevention

The Event Wagering System shall incorporate a mechanism to detect the use of remote desktop software, rootkits, virtualization, and/or any other programs identified as having the ability to circumvent location detection. This shall follow best practice security measures to:

a) Detect and block location data fraud (e.g., fake location apps, virtual machines, remote desktop programs, etc.) prior to completing each wager;
b) Examine the IP address upon each Remote Wagering Device connection to a network to ensure a known Virtual Private Network (VPN) or proxy service is not in use;
c) Detect and block devices which indicate system-level tampering (e.g., rooting, jailbreaking, etc.);
d) Stop "Man-In-The-Middle" attacks or similar hacking techniques and prevent code manipulation;
e) Utilize detection and blocking mechanisms verifiable to an application level; and
f) Monitor and prevent wagers placed by a single player account from geographically inconsistent locations (e.g., wager placement locations were identified that would be impossible to travel between in the time reported).

### 2.7.3 Location Detection for Remote Wagering on a WLAN

Where remote wagering occurs over a Wireless Local Area Network (WLAN), the Event Wagering System shall incorporate one of the following methods that can track the locations of all players connected to the WLAN:

a) A location detection service or application in which each player shall pass a location check prior to completing each wager. This service or application shall meet the requirements specified in the next section for "Location Detection for Remote Wagering Over the Internet"; or

b) A location detection component that detects in real-time when any players are no longer in the permitted area and prevent further wagers from being placed. This can be accomplished with the use of specific IT hardware such as directional antennas, Bluetooth sensors or other methods to be evaluated on a case-by-case basis by the independent test laboratory.

### 2.7.4 Location Detection for Remote Wagering Over the Internet

Where remote wagering occurs over the internet, the Event Wagering System shall incorporate a location detection service or application to reasonably detect and dynamically monitor the location of a player attempting to place a wager; and to monitor and enable the blocking of unauthorized attempts to place a wager.

a) Each player shall pass a location check prior to completing the first wager after logging in on a specific Remote Wagering Device. Subsequent location checks on that device shall occur prior to completing wagers after a period of 30 minutes since the previous location check, or as otherwise specified by the regulatory body:
   i. If the location check indicates the player is outside the permitted boundary or cannot successfully locate the player, the wager shall be rejected, and the player shall be notified of this.
   ii. An entry shall be recorded in a time stamped log any time a location violation is detected, including the unique player ID and the detected location.
b) A geolocation method shall be used to provide a player's physical location and an associated confidence radius. The confidence radius shall be entirely located within the permitted boundary.
c) Accurate location data sources (Wi-Fi, GSM, GPS, etc.) shall be utilized by the geolocation method to confirm the player's location. If a Remote Wagering Device's only available location data source is an IP Address, the location data of a mobile device registered to the player account may be used as a supporting location data source under the following conditions:
   i. The Remote Wagering Device (where the wager is being placed) and the mobile device shall be determined to be near one another.
   ii. If allowed by the regulatory body, carrier-based location data of a mobile device may be used if no other location data sources other than IP Addresses are available.
d) The geolocation method shall possess the ability to control whether the accuracy radius of the location data source is permitted to overlap or exceed defined buffer zones or the permitted boundary; and
e) To mitigate and account for discrepancies between mapping sources and variances in geospatial data, boundary polygons based on audited maps approved by the regulatory body as well as overlay location data onto these boundary polygons shall be utilized.

## 2.8 Information to be Maintained

### 2.8.1 Data Retention and Time Stamping

The Event Wagering System shall be capable of maintaining and backing up all recorded data as discussed within this section:

a) The system clock shall be used for all time stamping.

b) The system shall provide a mechanism to export the data for the purposes of data analysis and auditing/verification (e.g., CSV, XLS).

### 2.8.2 Wager Record Information

For each individual wager placed by the player, the information to be maintained and backed up by the Event Wagering System shall include:

a) The date and time the wager was placed;
b) Any player choices involved in the wager:
   i. Market and line postings (e.g., money line bet, point spreads, over/under amounts, win/place/show);
   ii. Wager selection (e.g., athlete or team name and number);
   iii. Any special condition(s) applying to the wager;
c) The results of the wager (blank until confirmed);
d) Total amount wagered, including any promotional/bonus credits (if applicable);
e) Total amount won, including any promotional/bonus credits (if applicable);
f) Commission or fees collected (if applicable);
g) The date and time the winning wager was paid to the player;
h) Unique identification number of the wager;
i) User identification or unique Wagering Device ID which issued the wager record (if applicable);
j) Relevant location information;
k) Event and market identifiers;
l) Current wager status (active, cancelled, unredeemed, pending, void, invalid, redemption in progress, redeemed, etc.);
m) Unique player ID, for wagers conducted using a player account;
n) Redemption period (if applicable); and
o) Open text field for attendant input of player description or picture file (if applicable);

### 2.8.3 Market Information

For each individual market available for wagering, the information to be maintained and backed up by the Event Wagering System shall include:

a) The date and time the wagering period started and ended;
b) The date and time the event started and ended or is expected to occur for future events (if known);
c) The date and time the results were confirmed (blank until confirmed);
d) Total amount of wagers collected, including any promotional/bonus credits (if applicable);
e) The line postings that were available throughout the duration of a market (time stamped) and the confirmed result (win/loss/push);
f) Total amount of winnings paid to players, including any promotional/bonus credits (if applicable);
g) Total amount of wagers voided or cancelled, including any promotional/bonus credits (if applicable);
h) Commission or fees collected (if applicable);

i) Event status (in progress, complete, confirmed, etc.); and
j) Event and market identifiers.

### 2.8.4 Contest/Tournament Information

For Event Wagering Systems which support contests/tournaments, the information to be maintained and backed up by the Event Wagering System shall include for each contest/tournament:

a) Name of the contest/tournament;
b) The date and time the contest/tournament occurred or will occur (if known);
c) Unique player ID and name of each registered player, amount of entry fee paid, and the date paid;
d) Unique player ID and name of each winning player, amount paid, and the date paid;
e) Total amount of entry fees collected, including any promotional/bonus credits (if applicable);
f) Total amount of winnings paid to players, including any promotional/bonus credits (if applicable);
g) Commission or fees collected (if applicable); and
h) Contest/tournament status (in progress, complete, etc.).

### 2.8.5 Player Account Information

For Event Wagering Systems which support player account management, the information to be maintained and backed up by the Event Wagering System shall include for each player account:

a) Unique player ID and player name;
b) Player data (including verification method);
c) The date of player agreement to the operator's terms and conditions and privacy policy;
d) Account details and current balance;
e) Open text field for attendant input of player description or picture file (if applicable);
f) Previous accounts, if any, and reason for de-activation;
g) The date and method from which the account was registered (e.g., remote vs. on-site);
h) The date and time of last log in;
i) Exclusions/limitations information as required by the regulatory body:
    i. The date and time of the request (if applicable);
    ii. Description and reason of exclusion/limitation;
    iii. Type of exclusion/restriction (e.g., operator-imposed exclusion, self-imposed limitation);
    iv. The date exclusion/limitation commenced;
    v. The date exclusion/limitation ended (if applicable);
j) Financial Transaction information:
    i. Type of transaction (e.g., deposit, withdrawal, adjustment);
    ii. The date and time of the transaction;
    iii. Unique transaction ID;
    iv. Amount of transaction;
    v. Total account balance before/after transaction;
    vi. Total amount of fees paid for transaction (if applicable);
    vii. User identification or unique Wagering Device ID which handled the transaction (if applicable);

viii. Transaction status (pending, complete, etc.);
ix. Method of deposit/withdrawal (e.g., cash, debit or credit card, personal check, cashier's check, wire transfer, money order);
x. Deposit authorization number; and
xi. Relevant location information.

### 2.8.6 Promotion/Bonus Information

For Event Wagering Systems which support promotions and/or bonuses that are redeemable for cash, wagering credits, or merchandise, the information to be maintained and backed up by the Event Wagering System shall include for each promotion/bonus:

a) The date and time the promotion/bonus period started and ended or will end (if known);
b) Current balance for promotion/bonus;
c) Total amount of promotions/bonuses issued;
d) Total amount of promotions/bonuses redeemed;
e) Total amount of promotions/bonuses expired;
f) Total amount of promotion/bonus adjustments; and
g) Unique ID for the promotion/bonus.

### 2.8.7 Wagering Device Information

For each individual Self-Service Wagering Device or POS Wagering Device, the information to be maintained and backed up by the Event Wagering System shall include, as applicable:

a) Unique Wagering Device ID;
b) Wager record purchases;
c) Winning wager record redemptions, if supported;
d) Wager record voids and cancellations; and
e) User identification and session information, for POS Wagering Devices;

### 2.8.8 Significant Event Information

Significant event information to be maintained and backed up by the Event Wagering System shall include:

a) Failed login attempts;
b) Program error or authentication mismatch;
c) Significant periods of unavailability of any critical component of the system;
d) Large wins (single and aggregate over defined time period) in excess of a value specified by the regulatory body, including wager record information;
e) Large wagers (single and aggregate over defined time period) in excess of a value specified by the regulatory body, including wager record information;
f) System voids, overrides, and corrections;
g) Changes to live data files occurring outside of normal program and operating system execution;
h) Changes that are made to the download data library, including the addition, changing or deletion

of software, where supported;
i) Changes to operating system, database, network, and application policies and parameters;
j) Changes to date/time on master time server;
k) Changes to previously established criteria for an event or market (not including line posting changes for active markets);
l) Changes to the results of an event or market;
m) Changes to promotion and/or bonus parameters;
n) Player Account Management:
    i. Adjustments to a player account balance;
    ii. Changes made to player data and sensitive information recorded in a player account;
    iii. Deactivation of a player account;
    iv. Large financial transactions (single and aggregate over defined time period) in excess of a value specified by the regulatory body, including transaction information;
o) Irrecoverable loss of sensitive information;
p) Any other activity requiring user intervention and occurring outside of the normal scope of system operation; and
q) Other significant or unusual events as deemed applicable by the regulatory body.

### 2.8.9 User Access Information

For each user account, the information to be maintained and backed up by the Event Wagering System shall include:

a) Employee name and title or position;
b) User identification;
c) Full list and description of functions that each group or user account may execute;
d) The date and time the account was created;
e) The date and time of last log in;
f) The date and time of last password change;
g) The date and time the account was disabled/deactivated; and
h) Group membership of user account (if applicable).

## 2.9 Reporting Requirements

### 2.9.1 General Reporting Requirements

The Event Wagering System shall be capable of generating the information needed to compile reports as required by the regulatory body. In addition to meeting the requirements in the section above for "Data Retention and Time Stamping", the following requirements shall apply for required reports:

a) The system shall be able to provide the reporting information on demand and for intervals required by the regulatory body including, but not limited to, daily, month-to-date (MTD), year-to-date (YTD), and life-to-date (LTD).
b) Each required report shall contain:
    i. The operator, the selected interval and the date/time the report was generated; and
    ii. An indication of "No Activity" or similar message if no information appears for the period

specified.

**NOTE:** In addition to the reports outlined in this section, the regulatory body may also require other reports utilizing the information stored under the "Information to be Maintained" section of this document.

### 2.9.2 Operator Revenue Reports

The Event Wagering System shall be able to provide the following information needed to compile one or more reports on operator revenue for each event as a whole and for each individual market within that event which may be used for operator taxation information:

a) The date and time each event started and ended;
b) Total amount of wagers collected;
c) Total amount of winnings paid to players;
d) Total amount of wagers voided or cancelled;
e) Commission and fees collected (if applicable);
f) Event and market identifiers; and
g) Event status (in progress, complete, confirmed, etc.).

### 2.9.3 Operator Liability Reports

The Event Wagering System shall be able to provide the following information needed to compile one or more reports on operator liability:

a) Total amount held by the operator for the player accounts (if applicable);
b) Total amount of wagers placed on future events; and
c) Total amount of winnings owed but unpaid by the operator on winning wagers.

### 2.9.4 Future Events Reports

The Event Wagering System shall be able to provide the following information needed to compile one or more reports on future events for the gaming day:

a) Wagers placed prior to the gaming day for future events (total and by wager);
b) Wagers placed on the gaming day for future events (total and by wager);
c) Wagers placed prior to the gaming day for events occurring on that same day (total and by wager);
d) Wagers placed on the gaming day for events occurring on that same day (total and by wager);
e) Wagers voided or cancelled on the gaming day (total and by wager); and
f) Event and market identifiers.

### 2.9.5 Significant Events and Alterations Reports

The Event Wagering System shall be able to provide the following information needed to compile one or more reports for each significant event or alteration as applicable:

a) The date and time of the significant event or alteration;
b) Event/component identification (if applicable);
c) Identification of user(s) who performed and/or authorized the significant event or alteration;
d) Reason/description of the significant event or alteration, including data or parameter altered;
e) Data or parameter value before alteration; and
f) Data or parameter value after alteration.

# Chapter 3: Wagering Device Requirements

## 3.1 Introduction

### 3.1.1 General Statement

A wager may be placed using one of the following types of Wagering Devices as allowed by the regulatory body. Any other types of Wagering Devices will be reviewed on a case-by-case basis, as allowed by the regulatory body.

a) Point-of-Sale (POS) Wagering Device: An attendant station that at a minimum will be used by an attendant for the execution or formalization of wagers placed on behalf of a player.
b) Self-Service Wagering Device: A kiosk that at a minimum will be used for the execution or formalization of wagers placed by a player directly and, if supported, may be used for redemption of winning wager records.
c) Remote Wagering Device: A player-owned device operated either on an in-venue wireless network or over the internet that at a minimum will be used for the execution or formalization of wagers placed by a player directly. Examples of a Remote Wagering Device include a personal computer, mobile phone, tablet, etc.

## 3.2 Wagering Software

### 3.2.1 General Statement

Wagering Software is used to take part in wagering and financial transactions with the Event Wagering System which, based on design, is downloaded to or installed on the Wagering Device, run from the Event Wagering System which is accessed by the Wagering Device, or a combination of the two.

### 3.2.2 Software Identification

Wagering Software shall contain sufficient information to identify the software and its version.

### 3.2.3 Software Validation

For Wagering Software installed locally on the Wagering Device, it shall be possible to authenticate that all critical components contained in the software are valid each time the software is loaded for use, and where supported by the system, on demand as required by the regulatory body. Critical components may include, but are not limited to, wagering rules, elements that control the communications between the Wagering Device and the Event Wagering System, or other components that are needed to ensure proper operation of the software. In the event of a failed authentication (i.e., program mismatch or authentication failure), the software shall prevent wagering operations and display an appropriate error message.

**NOTE:** Program verification mechanisms will be evaluated on a case-by-case basis and approved by the regulatory body and the independent test laboratory based on industry-standard security practices.

### 3.2.4 User Interface Requirements

The user interface is defined as an interface application or program through which the user views and/or interacts with the Wagering Software. The user interface shall meet the following requirements:

a) The functions of all buttons, touch or click points shall be clearly indicated within the area of the button, or touch/click point or within the help menu. There shall be no functionality available through any buttons or touch/click points on the user interface that are undocumented.
b) Any resizing or overlay of the user interface shall be mapped accurately to reflect the revised display and touch/click points.
c) User interface instructions, as well as information on the functions and services provided by the software, shall be clearly communicated to the user and shall not be misleading or inaccurate.
d) The display of the instructions and information shall be adapted to the user interface. For example, where a Wagering Device uses technologies with a smaller display screen, it is permissible to present an abridged version of the wagering rules accessible directly from within the wagering screen and make available the full/complete version of the wagering rules via another method, such as a secondary screen, help menu, or other interface that is easily identified on the visual wagering screen.

### 3.2.5 Simultaneous Inputs

Wagering Software shall not be adversely affected by the simultaneous or sequential activation of the various inputs and outputs which might, whether intentionally or not, cause malfunctions or invalid results.

### 3.2.6 Wager Record Printers

If the Wagering Device uses a printer to issue printed wager records to the player, the printed wager record shall include information as indicated in "Wager Record" section of this document. It may be permissible for some of this information to be contained on the ticket stock itself.

### 3.2.7 Communications

Wagering Software shall be designed or programmed such that it may only communicate with authorized components through secure communications. If communication between the Event Wagering System and the Wagering Device is lost, the software shall prevent further wagering operations and display an appropriate error message. It is permissible for the software to detect this error when the device tries to communicate with the system.

## 3.3 Self-Service Wagering Devices

### 3.3.1 General Statement

A player places a wager at a Self-Service Wagering Device by using funds from their player account or by using peripheral devices as authorized by the regulatory body. In addition to the requirements for "Wagering Software", the applicable requirements established within the *GLI-20 Standards for Kiosks* and other applicable jurisdictional requirements observed by the regulatory body shall be met for all proprietary components of the Self-Service Wagering Device.

## 3.4 POS Wagering Devices

### 3.4.1 General Statement

A player places a wager at POS Wagering Device by using funds from their player account or by providing payment for the wager(s) directly to the attendant. In addition to the requirements for "Wagering Software", the requirements established in this section shall be met for POS Wagering Devices.

### 3.4.2 Touch Screen Displays

Touch screen displays, if in use by the Wagering Software, shall be accurate, and if required by their design, shall support a calibration method to maintain that accuracy; alternatively, the display hardware may support automatic self-calibration.

### 3.4.3 Printing Wager Records

If the POS Wagering Device connects to a printer to produce printed wager records and/or wagering instruments (vouchers and coupons), the printer and/or Wagering Software shall be able to detect and indicate the following error conditions, where supported. It is permissible for the error condition to be detected when it tries to print:

a) Low battery (where power is external to the POS Wagering Device);
b) Out of paper/paper low; and
c) Printer disconnected.

### 3.4.4 Wireless POS Wagering Devices

For wireless POS Wagering Devices, the applicable requirements for "Client-Server Interactions" of the next section shall also be met. Additionally, communication shall only occur between the wireless POS Wagering Device and the Event Wagering System via authorized access points within the venue.

## 3.5 Remote Wagering Devices

### 3.5.1 General Statement

A player may only place a wager on a Remote Wagering Device by using funds from their player account (i.e. anonymous wagering transactions are prohibited). Depending on the implementation(s)

authorized by the regulatory body, Remote Wagering Devices may be used on an in-venue Wireless Local Area Network (WLAN) or over the internet. In addition to the requirements for "Wagering Software", the requirements established in this section shall be met for Remote Wagering Devices.

### 3.5.2 Client-Server Interactions

The player may obtain/download an application or software package containing the Wagering Software or access the software via a browser to take part in wagering and financial transactions with the Event Wagering System.

a) Players shall not be able to use the software to transfer data to one another, other than chat functions (e.g., text, voice, video, etc.) and approved files (e.g., user profile pictures, photos, etc.);
b) The software shall not automatically alter any device-specified firewall rules to open ports that are blocked by either a hardware or software firewall;
c) The software shall not access any ports (either automatically or by prompting the user to manually access) which are not necessary for the communication between the Remote Wagering Device and the server;
d) If the software includes additional non-wagering related functionality, this additional functionality shall not alter the software's integrity in any way;
e) The software shall not possess the ability to override the volume settings of the Remote Wagering Device; and
f) The software shall not be used to store sensitive information. It is recommended that auto complete, password caching, or other methods that will fill in the password field are disabled by default for the software.

### 3.5.3 Compatibility Verification

During any installation or initialization and prior to commencing wagering operations, the Wagering Software used in conjunction with the Event Wagering System shall detect any incompatibilities or resource limitations with the Remote Wagering Device that would prevent proper operation of the software (e.g., software version, minimum specifications not met, browser type, browser version, plug-in version, etc.). If any incompatibilities or resource limitations are detected the software shall prevent wagering operations and display an appropriate error message.

### 3.5.4 Software Content

Wagering Software shall not contain any malicious code or functionality deemed to be malicious in nature by the regulatory body. This includes, but is not limited to, unauthorized file extraction/transfers, unauthorized device modifications, unauthorized access to any locally stored personal information (e.g., contacts, calendar, etc.) and malware.

### 3.5.5 Cookies

Where cookies are used, players shall be informed of the cookie use upon Wagering Software installation or during player registration. When cookies are required for wagering, wagering cannot occur if they are not accepted by the Remote Wagering Device. All cookies used shall contain no

malicious code.

### 3.5.6 Information Access

The Wagering Software shall be able to display, either directly from the user interface or from a page accessible to the player, the items specified in the following sections of this document. For Remote Wagering Devices which only allow wagers within a venue, it is acceptable to disclose to the player the means of obtaining the information required by this section:

a) "Wagering Rules and Content";
b) "Player Protection Information";
c) "Terms and Conditions";
d) "Privacy Policy";
e) "Wagering Displays and Information"; and
f) "Results Display".

**NOTE:** It is accepted that the system will unavoidably be subject to a certain degree of synchronization delay for updates to this information as displayed on the software, and it is possible that information may only be updated at the player's next interaction with the software which causes the on-screen information to be refreshed.

# Chapter 4: Event Wagering Requirements

## 4.1 Introduction

### 4.1.1 General Statement

This chapter sets forth technical requirements for wagering operations, including, but not limited to rules for wager placement and results for markets within an event.

## 4.2 Wagering Displays and Information

### 4.2.1 Posting of Wagering Rules

Comprehensive wagering rules shall be posted by an operator for the markets and event types currently offered. Where the Wagering Software includes these wagering rules directly, the software will be evaluated against the requirements within the "Wagering Rules and Content" section of this document.

### 4.2.2 Dynamic Wagering Information

The following information shall be made available without the need for placing a wager. Within a venue this information may be displayed on a Wagering Device and/or an external display.

a) Information regarding the events and markets available for wagering;
b) Current odds/payouts and prices for available markets;
c) For types of markets where individual wagers are gathered into pools:
   i. Up-to-date odds/payouts information for simple market pools. For complex market pools, it is accepted that there may be reasonable limitations to the up-to-date accuracy of the pool estimates displayed to the player;
   ii. Up-to-date values of total investments for all market pools; and
   iii. The dividends of any decided market.

**NOTE:** This information shall be displayed as accurately as possible within the constraints of communication delays and latencies.

### 4.2.3 Player Resources/Features

Where allowed by the regulatory body, player resources/features may be provided such as one that offers advice, hints, or suggestions to a player, or a data stream that may be used to externally facilitate wager selection, if they conform to the following requirements:

a) The player shall be made aware of each resource/feature that is available, the advantage it offers (if any), and the options that exist for selection.
b) The method for obtaining each resource/feature shall be disclosed to the player. Any player resources/features that are offered to the player for purchase shall clearly disclose the cost.

c) The availability and functionality of player resources/features shall remain consistent for all players.
d) For peer-to-peer wagering, the player shall be provided with sufficient information to make an informed decision, prior to participation, as to whether to participate with player(s) who may possess such resources/features.

## 4.3 Wager Placement

### 4.3.1 General Statement

Wagers are placed in conjunction with a player account or by funds provided to a Wagering Device or an attendant. Depending on the type of Wagering Device, wagers may be placed directly by the player or on behalf of a player by an attendant.

**NOTE:** Wagers placed using a Remote Wagering Device may only be placed in conjunction with a player account.

### 4.3.2 Placement of a Wager

The following rules only apply to the placement of a paid wager directly by a player on the Wagering Device:

a) The method of placing a wager shall be straightforward, with all selections (including their order, if relevant) identified. When the wager involves multiple events (e.g., parlays), such groupings shall be identified.
b) Players shall have the ability to select the market they want to place a wager on.
c) Wagers shall not be automatically placed on behalf of the player without the player's consent/authorization.
d) Players shall have an opportunity to review and confirm their selections before the wager is submitted. This does not preclude the use of "single-click" wagering where permitted by the regulatory body and opted in by the player.
e) Situations shall be identified where the player has placed a wager for which the associated odds/payouts or prices have changed, and unless the player has opted in to auto-accept changes as permitted by the regulatory body, provide a notification to confirm the wager given the new values.
f) Clear indication shall be provided that a wager has been accepted or rejected (in full or in part). Each wager shall be acknowledged and clearly indicated separately so that there is no doubt as to which wagers have been accepted.
g) For wagers conducted using a player account:
    i. The account balance shall be readily accessible.
    ii. A wager shall not be accepted that could cause the player to have a negative balance.
    iii. The account balance is to be debited when the wager is accepted by the system.

### 4.3.3 Automatic Acceptance of Changes in Wagers

Where allowed by the regulatory body, an Event Wagering System may support a feature that allows a player while placing a wager to auto-accept changes in odds/payouts or price of the wager provided that it conforms to the following requirements:

a) Any auto-accept options available (e.g., auto-accepting all wagers with higher price, auto-accepting all wagers with lower price, etc.) shall be explained to the player;
b) The player shall manually opt in to use this functionality (i.e., it shall not be set by default); and
c) The player shall be able to opt out at any time.

### 4.3.4 Wager Record

Upon completion of a wagering transaction, the player shall have access to a wager record which contains the following information:

a) The date and time the wager was placed;
b) The date and time the event is expected to occur (if known);
c) Any player choices involved in the wager:
    i. Market and line postings (e.g., money line bet, point spreads, over/under amounts, win/place/show, etc.);
    ii. Wager selection (e.g., athlete or team name and number);
    iii. Any special condition(s) applying to the wager;
d) Total amount wagered, including any promotional/bonus credits (if applicable);
e) Unique identification number and/or barcode of the wager;
f) User identification or unique Wagering Device ID which issued the wager record (if applicable);
g) Venue Name/Site Identifier (for printed wager record, it is permissible for this information to be contained on the ticket stock itself); and
h) Redemption period (for printed wager records it is permissible for this information to be contained on the ticket stock itself).

**NOTE:** Some of the above-listed information may also be part of the unique identification number and/or barcode. Multiple barcodes are allowed and may represent more than just the unique identification number.

### 4.3.5 Wagering Period Close

It shall not be possible to place wagers once the wagering period has closed.

### 4.3.6 Free Play Mode

Where allowed by the regulatory body, the Event Wagering System may support free play mode, which allows a player to participate in wagering without paying. Free play mode shall not mislead the player about the odds/payouts available in the paid version.

## 4.4 Results and Payment

### 4.4.1 Results Display

Results entry shall include the entry of all information which may affect the outcome of all types of wagers offered for that event.

a) It shall be possible for a player to obtain the results of their wagers on any decided market once the results have been confirmed.
b) Any change of results (e.g., due to statistics/line corrections) shall be made available.

### 4.4.2 Payment of Winnings

Once the results of the event are entered and confirmed, the player may receive payment for their winning wagers. This does not preclude the ability for the player to perform a redemption for an adjusted payout before event conclusion where offered and allowed by the regulatory body.

### 4.4.3 Winning Wager Record Redemption

The following requirements apply to the redemption of a winning wager at a Wagering Device, as allowed by the regulatory body. This section does not apply to winning wagers tied to a player account which automatically updates the account balance.

a) The Event Wagering System shall process winning wager record redemption according to the secure communication protocol implemented.
b) No winnings are issued to the player prior to confirmation of winning wager record validity.
c) The Event Wagering System shall have the ability to identify and provide a notification in the case of invalid or unredeemable wager records for the following conditions:
    i. Wager record cannot be found on file;
    ii. Wager record is not a winner;
    iii. Winning wager record has already been paid; or
    iv. Amount of winning wager record differs from amount on file (requirement can be met by display of winning wager amount for confirmation during the redemption process).
d) The Event Wagering System shall update the wager record status on the database during each phase of the redemption process accordingly. In other words, whenever the wager record status changes, the system shall update the database.

## 4.5 Virtual Event Wagering

### 4.5.1 General Statement

Virtual event wagering allows for the placement of wagers on simulations of sporting events, contests, and races whose results are based solely on the output of an approved Random Number Generator (RNG) as allowed by the regulatory body. The following requirements are only applicable to cases that virtual event wagering is conducted in total by the Event Wagering System where a wager is placed at a Wagering Device or through interaction with an attendant and then the virtual event is displayed via a public or common display (e.g. external display, website, etc.). For virtual events conducted by a gaming device (e.g., player makes a wager and the event plays out before them on their machine or a shared display on a multi-player machine), please refer to the *GLI-11 Standards for Gaming Devices* or other jurisdictional requirements observed by the regulatory body.

### 4.5.2 Randomization and Virtual Events

A cryptographic RNG shall be utilized to determine virtual event outcomes and shall comply with the applicable jurisdictional requirements set out for RNGs. In the absence of specific jurisdictional standards, the "Random Number Generator (RNG) Requirements" chapter of the *GLI-11 Standards for Gaming Devices* shall be used as applicable. Additionally, the evaluation of virtual event outcomes using an RNG shall comply with the following rules:

a) Where more than one RNG is used to determine different virtual event outcomes, each RNG shall be separately evaluated; and
b) Where each instance of an RNG is identical, but involves a different implementation within the virtual event, each implementation shall be separately evaluated.

### 4.5.3 Virtual Event Selection Process

Determination of events of chance that result in a monetary award shall not be influenced, affected, or controlled by anything other than the values selected by an approved RNG, in accordance with the following requirements:

a) It shall not be possible to ascertain the outcome of the virtual event prior to its commencement;
b) When making calls to the RNG, the virtual event shall not limit the outcomes available for selection, except as provided for by design;
c) The virtual event shall not modify or discard outcomes selected by the RNG due to adaptive behavior. Additionally, outcomes shall be used as described by the rules of the virtual event;
d) After the commencement of a virtual event, no further actions or decisions may be made that change the behavior of any of the elements of chance within the virtual event, other than player decisions;
e) Except as provided for by the rules of the virtual event, events of chance shall be independent and shall not correlate with any other events within the same virtual event, or events within previous virtual events;
f) Any associated equipment used in conjunction with an Event Wagering System shall not influence or modify the behaviors of the system's RNG and/or random selection process, except as authorized, or intended by design;
g) Virtual event outcomes shall not be affected by the effective bandwidth, link utilization, bit error rate or other characteristics of the communications channel between the Event Wagering System and the Wagering Device; and
h) Wagering Software shall not contain any logic utilized to generate the result of any virtual event. All critical functions including the generation of any virtual event shall be generated by the Event Wagering System and be independent of the Wagering Device.

### 4.5.4 Virtual Event Display

Displays for a virtual event shall conform to applicable display requirements of this standard. In addition, the following display requirements apply:

a) Statistical data that is made available to the player pertaining to the virtual event shall not misrepresent the capabilities of any virtual participant. This does not prevent the use of an element of chance or randomness from impacting performance of the virtual participant during the virtual event.
b) For scheduled virtual events, a countdown of the time remaining to place a wager in that event shall be displayed to the player. It shall not be possible to place wagers on the event once this time has passed; however, this requirement does not prohibit the implementation of in-play wagers.
c) Each virtual participant shall be unique in appearance, where applicable to the wager. For instance, if the wager is on one team to beat another, the virtual participants themselves do not need to be unique in appearance, however the teams that they are on shall be visually distinct from each other.
d) The result of a virtual event shall be clear, unambiguous, and displayed for a sufficient length of time to allow a player a reasonable opportunity to verify the virtual event's outcome.

### 4.5.5 Simulation of Physical Objects

Where a virtual event incorporates a graphical representation or simulation of a physical object that is used to determine virtual event outcome, the behaviors portrayed by the simulation shall be consistent with the real-world object, unless otherwise denoted by the virtual event rules. This requirement does not apply to graphical representations or simulations that are utilized for entertainment purposes only. The following shall apply to the simulation:

a) The probability of any event occurring in the simulation that affects the outcome of the virtual event shall be analogous to the properties of the physical object;
b) Where the virtual event simulates multiple physical objects that would normally be expected to be independent of one another based on the rules of the virtual event, each simulation shall be independent of any other simulation; and
c) Where the virtual event simulates physical objects that have no memory of previous events, the behavior of the simulated objects shall be independent of their previous behavior, so as to be non-adaptive and non-predictable, unless otherwise disclosed to the player.

### 4.5.6 Physics Engine

Virtual events may utilize a "physics engine" which is specialized software that approximates or simulates a physical environment, including behaviors such as motion, gravity, speed, acceleration, inertia, trajectory, etc. A physics engine shall be designed to maintain consistent play behaviors and virtual event environment unless an indication is otherwise provided to the player by the virtual event rules. A physics engine may utilize the random properties of an RNG to impact virtual event outcome.

**NOTE:** Implementations of a physics engine in a virtual event will be evaluated on a case-by-case basis by the independent test laboratory.

## 4.6 External Wagering Systems

### 4.6.1 General Statement

This section contains requirements for the circumstances where the Event Wagering System communicates with an external wagering system in any of the following configurations:

a) The Event Wagering System is acting as the "host wagering system" receiving, for its own markets, wagers from one or more external "guest wagering systems"; or
b) The Event Wagering System is acting as a "guest wagering system" passing wagers to an external "host wagering system," for that system's markets.

**NOTE:** The requirements of this section apply to the interoperability of the Event Wagering System with the external wagering system and are not a complete evaluation of the external wagering system itself. The external wagering system may independently be subject to evaluation by the independent test laboratory per regulatory body discretion.

### 4.6.2 Information

The following requirements apply to information being conveyed between the host wagering system and the guest wagering system:

a) If the host wagering system provides pari-mutuel wagering for the guest wagering system, the Event Wagering System shall be able to:
   i. When acting as the guest wagering system, receive the current dividends for active pools sent from the host wagering system.
   ii. When acting as the host wagering system, pass the current dividends for active pools to all receiving guest wagering systems.
b) If the host wagering system provides fixed odds wagering for the guest wagering system where the odds/payouts and prices can be dynamically changed, the Event Wagering System shall be able to:
   i. When acting as the guest wagering system, receive the current odds/payouts and prices sent from the host wagering system whenever any odds/payouts and prices are changed.
   ii. When acting as the host wagering system, pass the current odds/payouts and prices to all receiving guest wagering systems whenever any odds/payouts and prices are changed.
c) Change of event status information shall be passed from the host wagering system to the guest wagering system whenever any change occurs, including:
   i. Withdrawn/reinstated selections;
   ii. Altered event starting time;
   iii. Individual markets opened/closed;
   iv. Results entered/modified;
   v. Results confirmed; and
   vi. Event cancelled.

### 4.6.3 Wagers

The following requirements apply to wagers being placed between the host wagering system and the guest wagering system:

a) Wagers placed on the guest wagering system shall receive clear acknowledgment of acceptance, partial acceptance (including details), or rejection sent by the host wagering system.
b) If the cost of the wager is determined by the host wagering system, there shall be a positive confirmation sequence in place to enable the player to accept the wager cost and the guest wagering system to determine that there are enough funds in the account balance to meet the wager cost prior to making an offer to the host wagering system.
c) Where wagers may be placed in bulk, the following requirements apply:
    i. If the stream of wagers is interrupted for any reason, there shall be a means available to determine where in the stream that the interruption occurred.
    ii. No wager in the stream may be greater than the account balance. If such a wager is attempted, the entire stream is to be halted.
d) The account balance shall be debited an amount equaling the offer and cost to the host wagering system. The funds shall remain as a pending transaction with details of the offer to the host wagering system logged. On receipt of acknowledgment from the host wagering system, the appropriate adjustments shall be made to the "pending" account and the account balance on the guest wagering system.
e) Cancellation requests from the guest wagering system shall receive clear acknowledgment of acceptance or rejection by the host wagering system. The player is not to be credited by the guest wagering system until final confirmation is received from the host wagering system including the amount of the voided or cancelled wager.

### 4.6.4 Results

When results are entered and confirmed on the host wagering system, each winning wager shall be transferred to the guest wagering system with the amount of the win. Confirmation of receipt of the winning wagers shall be acknowledged by the guest wagering system.

# Appendix A: Operational Audit for Wagering Procedures and Practices

## A.1 Introduction

### A.1.1 General Statement

This appendix sets forth procedures and practices for wagering operations which will be reviewed in an operational audit as a part of the Event Wagering System evaluation, including, but not limited to establishing wagering rules, suspending events, handling various wagering and financial transactions, creating markets, settling wagers, closing markets, cancellations of events, voiding or cancelling wagers, player account management, fundamental practices relevant to the limitation of risks, and any other objectives established by the regulatory body.

**NOTE:** It is also recognized that additional procedures and practices which are not specifically included within this standard will be relevant and required for an operational audit as determined by the operator and/or regulatory body within their rules, regulations, and Minimum Internal Control Standards (MICS).

## A.2 Internal Control Procedures

### A.2.1 Internal Control Procedures

The operator shall establish, maintain, implement and comply with internal control procedures for wagering operations, including performing wagering and financial transactions.

### A.2.2 Information Management

The operator's internal controls shall include the processes for maintaining the recorded information specified under the section entitled "Information to be Maintained" for a period of five years or as otherwise specified by the regulatory body.

### A.2.3 Risk Management

The operator's internal controls shall contain details on its risk management framework, including but not limited to:

a) Automated and manual risk management procedures;
b) Employee management, including access controls and segregation of duties;
c) Information regarding identifying and reporting fraud and suspicious conduct;
d) Controls ensuring regulatory compliance;
e) Description of Anti-Money Laundering (AML) compliance standards including procedures for detecting structuring to avoid reporting requirements;
f) Description of all software applications that comprise the Event Wagering System;
g) Description of all types of wagers available to be offered by the operator;

h) Description of the method to prevent past-post wagers from being placed;
i) Description of all integrated third-party service providers; and
j) Any other information required by the regulatory body.

### A.2.4 Restricted Players

The operator's internal controls shall describe the method to prevent players from wagering on events in which they might have insider information, including, but not limited to the following examples, as required by the regulatory body:

a) Players identified as employees, subcontractors, directors, owners, and officers of an operator, as well as those within the same household, shall not place wagers on any event, except in private pools where their association with the operator is clearly disclosed.
b) Players identified as professional or collegiate athletes, team employees and owners, coaches, managers, handlers, athletic trainers, league officials and employees, referees, umpires, sports agents, and employees of a player or referee union, as well as those within the same household, shall not place wagers on any event in the sport in which they participate, or in which the athlete they represent participates.

## A.3 Player Account Controls

### A.3.1 Registration and Verification

Where player account registration is done manually by the operator, procedures shall be in place to satisfy the requirements for "Registration and Verification" as indicated within this document.

### A.3.2 Fraudulent Accounts

The operator shall have a documented public policy for the treatment of player accounts discovered to being used in a fraudulent manner, including but not limited to:

a) The maintenance of information about any account's activity, such that if fraudulent activity is detected, the operator has the necessary information to take appropriate action;
b) The suspension of any account discovered to be engaged in fraudulent activity, such as a player providing access to underage persons; and
c) The handling of deposits, wagers, and wins associated with a fraudulent account.

### A.3.3 Terms and Conditions

A set of terms and conditions shall be available to the player. During the registration process and when any terms and conditions are materially updated (i.e. beyond any grammatical or other minor changes), the player shall agree to the terms and conditions. The terms and conditions shall:

a) State that only individuals legally permitted by their respective jurisdiction can participate in wagering;
b) Advise the player to keep their authentication credentials (e.g., password and username) secure;

c) Disclose all processes for dealing with lost authentication credentials, forced password changes, password strength and other related items;
d) Specify the conditions under which an account is declared inactive and explain what actions will be undertaken on the account once this declaration is made; and
e) Clearly define what happens to the player's pending wagers placed prior to any self-imposed or operator-imposed exclusion, including the return of all wagers, or settling all wagers, as appropriate.

### A.3.4 Privacy Policy

A privacy policy shall be available to the player. During the registration process and when the privacy policy is materially updated (i.e. beyond any grammatical or other minor changes), the player shall agree to the privacy policy. The privacy policy shall state

a) The player data required to be collected;
b) The purpose for information collection;
c) The period in which the information is stored;
d) The conditions under which information may be disclosed; and
e) An affirmation that measures are in place to prevent the unauthorized or unnecessary disclosure of the information.

### A.3.5 Player Data Security

Any information obtained in respect to the player account, including player data, shall be done in compliance with the privacy policy and local privacy regulations and standards observed by the regulatory body. In addition:

a) Any player data which is not subject to disclosure pursuant to the privacy policy shall be kept confidential, except where the release of that information is required by law.
b) There shall be procedures in place for the security and sharing of player data, funds in a player account and other sensitive information as required by the regulatory body, including, but not limited to:
    i. The designation and identification of one or more employees having primary responsibility for the design, implementation and ongoing evaluation of such procedures and practices;
    ii. The procedures to be used to determine the nature and scope of all information collected, the locations in which such information is stored, and the storage devices on which such information may be recorded for purposes of storage or transfer;
    iii. The measures to be utilized to protect information from unauthorized access; and
    iv. The procedures to be used in the event the operator determines that a breach of data security has occurred, including required notification to the regulatory body.

### A.3.6 Financial Transactions

Procedures shall be in place to ensure all financial transactions are conducted in accordance with local commerce regulations and requirements mandated by the regulatory body:

a) Where financial transactions cannot be performed automatically by the Event Wagering System, procedures shall be in place to satisfy the requirements for "Player Funds Maintenance" as indicated within this document.
b) Positive player identification or authentication shall be completed before the withdrawal of any funds can be made by the player.
c) A player's request for withdrawal of funds (i.e., deposited and cleared funds and wagers won) shall be completed by the operator within a reasonable amount of time, unless there is a pending unresolved player complaint/dispute or investigation. Such investigation shall be documented by the operator and available for review by the regulatory body.
d) The operator shall have security or authorization procedures in place to ensure that only authorized adjustments can be made to player accounts, and these changes are auditable.

### A.3.7 Limitations

Players shall be provided with a method to impose limitations for wagering parameters including, but not limited to deposits and wagers as required by the regulatory body. In addition, there shall be a method for the operator to impose any limitations for wagering parameters as required by the regulatory body.

a) Once established by a player and implemented by the operator, it shall only be possible to reduce the severity of self-imposed limitations upon 24 hours' notice, or as required by the regulatory body;
b) Players shall be notified in advance of any operator-imposed limits and their effective dates. Once updated, operator-imposed limits shall be consistent with what is disclosed to the player; and
c) Upon receiving any self-imposed or operator-imposed limitation order, the operator shall ensure that all specified limits are correctly implemented immediately or at the point in time (e.g., next login, next day) clearly indicated to the player.

### A.3.8 Exclusions

Players shall be provided with a method to exclude themselves from wagering for a specified period or indefinitely, as required by the regulatory body. In addition, there shall be a method for the operator to exclude a player from wagering as required by the regulatory body.

a) Players shall be given a notification containing exclusion status and general instructions for resolution where possible;
b) Immediately upon receiving the exclusion order, no new wagers or deposits are accepted from that player, until the exclusion has been removed;
c) While excluded, the player shall not be prevented from withdrawing any or all of their account balance, provided that the operator acknowledges that the funds have cleared, and that the reason(s) for exclusion would not prohibit a withdraw; and
d) All advertising or marketing material shall not specifically target players that have been excluded from play.

### A.3.9 Inactive Accounts

A player account is considered to be inactive under the conditions as specified in the terms and conditions. Procedures shall be in place to:

a) Protect inactive player accounts that contain funds from unauthorized access, changes or removal; and
b) Deal with unclaimed funds from inactive player accounts, including returning any remaining funds to the player where possible.

## A.4 General Operating Procedures

### A.4.1 Operator Reserves

The operator shall have processes in place for maintaining and protecting adequate cash reserves, as determined by the regulatory body, including segregated accounts of funds held for player accounts and operational funds such as those used to cover unclaimed winning wagers, potential winning wagers for the gaming day, etc.

### A.4.2 Protection of Player Funds

The operator shall have processes in place to ensure funds in an operator account are either to be held in trust for the player in a special purpose segregated account that is maintained and controlled by a properly constituted corporate entity that is not the operator and whose governing board includes one or more corporate directors who are independent of the operator and of any corporation related to or controlled by the operator. In addition, the operator shall have procedures that are reasonably designed to:

a) Ensure that funds generated from wagering are safeguarded and accounted for;
b) Make clear that the funds in the segregated account do not belong to the operator and are not available to creditors other than the player whose funds are being held; and
c) Prevent commingling of funds in the segregated account with other funds including, without limitation, funds of the operator.

### A.4.3 Taxation

The operator shall have a process in place to identify all wins that are subject to taxation (single wins or aggregate wins over a defined period as required) and provide the necessary information in accordance with each regulatory body's taxation requirements.

**NOTE:** Amounts won that exceed any jurisdictional specified limit shall require the appropriate documentation to be completed before the winning player is paid.

### A.4.4 Complaint/Dispute Process

The operator shall provide a method for a player to make a complaint/dispute, and to enable the player to notify the regulatory body if such complaint/dispute has not been or cannot be addressed by the operator, or under other circumstances as specified by the law of the regulatory body.

a) Players shall be able to log complaints/disputes on a 24/7 basis.
b) Records of all correspondence relating to a complaint/dispute shall be maintained for a period of five years or as otherwise specified by the regulatory body.
c) A documented process shall exist between the operator and the regulatory body on the complaint/dispute reporting and resolution process.

### A.4.5 Player Protection Information

Player protection information shall be available to the player. The player protection information shall contain at a minimum:

a) Information about potential risks associated with excessive wagering, and where to get help for a gambling problem;
b) A statement that no underage persons are permitted to participate in wagering;
c) A list of the available player protection measures that can be invoked by the player, such as self-imposed exclusion, and information on how to invoke those measures;
d) For player accounts, mechanisms in place which can be used to detect unauthorized use of their account, such as reviewing credit card statements against known deposits;
e) Contact information or other means for reporting a complaint/dispute; and
f) Contact information for the regulatory body and/or a link to their website.

## A.5 Wagering Rules and Content

### A.5.1 Wagering Rules

Wagering rules refers to any written, graphical, and auditory information provided to the public regarding event wagering operations. The operator shall adopt, and adhere to comprehensive wagering rules which shall be approved by the regulatory body:

a) Wagering rules shall be complete, unambiguous, and not misleading or unfair to the player.
b) Wagering rules that are presented aurally (via sound or voice) shall also be displayed in written form.
c) Wagering rules shall be rendered in a color that contrasts with the background color to ensure that all information is clearly visible/readable.
d) The operator shall keep a log of any changes to the wagering rules relating to placing wagers.
e) Where wagering rules are altered for events or markets being offered, all rule changes shall be time and date stamped showing the rule applicable in each period. If multiple rules apply to an event or market, the operator shall apply the rules that were in place when the wager was accepted.

### A.5.2 Wagering Rules Content

The following information shall be made available to the player. For wagers placed within a venue, it is acceptable for this information to be displayed by the Wagering Device directly or by external signage, forms, or brochures available:

a) The methods of funding a wager or player account, including a clear and concise explanation of all fees (if applicable);
b) As allowed by the regulatory body, any prizes that are offered in the form of merchandise, annuities, lump sum payments, or payment plans instead of cash payouts for each market that is offering such a prize;
c) The procedures by which any unrecoverable malfunctions of hardware/software are addressed including if this process results in the voiding or cancelling of any wagers; and
d) The procedures to deal with interruptions caused by the discontinuity of data flow from the network server during an event.
e) Rules of participation, including all wagering eligibility and scoring criteria, available events and markets, types of wagers accepted, line postings, all advertised awards, and the effect of schedule changes;
f) Payout information, including possible winning positions, rankings, and achievements, along with their corresponding payouts, for any available wager option;
g) Any restrictive features of wagering, such as wager amounts or maximum win values;
h) A description on restricted players, including any applicable limitations on wagering for them (e.g. athletes shall not wager on their sport);
i) The procedures for handling incorrectly posted events, markets, odds/payouts, prices, wagers, or results;
j) A wager cancellation policy which shall cater for wagers with multiple events (e.g., parlays) and indicate any prohibitions of voiding or cancelling wagers (e.g., after a fixed time period);
k) Whether the odds/payouts are locked-in at the time of the wager, or if the odds/payouts may change dynamically prior to the commencement of the event and the method of noticing changes to the odds/payouts;
l) For types of wagers where the odds/payouts are fixed at the time the wager is placed, any situations where the odds/payouts may be adjusted such as atypical winning outcomes (e.g., dead heats), cancelled legs of wagers with multiple events (e.g., parlays), and prorating;
m) For types of wagers where individual wagers are gathered into pools, the rules for dividend calculation including the prevailing formula for pool allocations and the stipulations of the event being wagered upon as approved by the regulatory body;
n) For in-play wagering, due to varying communication speeds or broadcast transmission latencies:
    i. Updates of the displayed information may put a player at a disadvantage to others who may have more up-to-date information; and
    ii. There may be delays incorporated in the registered time of an in-play wager to prevent past-post wagers and cancellations.
o) A statement that the operator reserves the right to:
    i. Refuse any wager or part of a wager or reject or limit selections prior to the acceptance of a wager for reasons indicated to the player in these rules;
    ii. Accept a wager at other than posted terms; and
    iii. Close wagering periods at their discretion;
p) If prizes are to be paid for combinations involving participants other than solely the first-place finisher (e.g., in an Olympic competition), the order of the participants that can be involved with these prizes (e.g., result 8-4-7);
q) The rules for any exotic wagering options (e.g., perfecta, trifecta, quinella, etc.) and the expected payouts;

r) What is to occur when an event or market is cancelled or withdrawn, including the handling of selections wagers with multiple events (e.g., parlays) where one or more of these legs are cancelled or withdrawn;
s) How a winning wager is determined and the handling of an award in any case where a tie is possible;
t) The payment of winning wagers, including the redemption period and the method for calculation. Where the calculation of payouts may involve rounding, information on how these circumstances are handled shall clearly explain:
    i. Rounding up, down (truncation), true rounding; and
    ii. Rounding to what level (e.g., 5 cents).

### A.5.3 Promotions and/or Bonuses

Players shall be able to access information in the wagering rules pertaining to any available promotions and/or bonuses, including how the player is notified when they have received a promotional award or bonus win and the terms of their withdrawal. This information shall be clear and unambiguous, especially where promotions or bonuses are limited to certain events, markets, or when other specific conditions apply.

### A.5.4 Contests/Tournaments

A contest/tournament, which permits a player to either purchase or be awarded the opportunity to engage in competitive wagering against other players, may be permitted provided the following rules are met:

a) Rules shall be made available to a player for review prior to contest/tournament registration. The rules shall include at a minimum:
    i. All conditions registered players shall meet to qualify for entry and advancement through, the contest/tournament;
    ii. Specific information pertaining to any single contest/tournament, including the available prizes or awards and distribution of funds based on specific outcomes; and
    iii. The name of the organization (or persons) that conducted the contest/tournament on behalf of, or in conjunction with, the operator (if applicable).
b) Procedures shall be in place to record the results of each contest/tournament and make publicly available for the registered players to review for a reasonable period of time. Subsequent to being posted publicly, the results of each contest/tournament shall be made available upon request. The results include the following:
    i. Name of the contest/tournament;
    ii. Date(s)/times(s) of the contest/tournament;
    iii. Total number of entries;
    iv. Amount of entry fees;
    v. Total prize pool; and
    vi. Amount paid for each winning category.

**NOTE:** For free contests/tournaments (i.e., registered player does not pay an entry fee), the information required by the above shall be recorded except for the number of entries, amount of entry fees and total prize pool.

## A.6 Wagering Procedures and Controls

### A.6.1 Odds/Payouts and Prices

There shall be established procedures for setting and updating the odds/payouts and prices including publicly providing the current odds/payouts and prices, changing odds/payouts and prices as necessary to handle exceptions, and properly logging and periodically logging the odds/payouts and prices.

### A.6.2 Statistics/Line Data

The operator shall ensure that any statistics/line data that is made available to the player pertaining to an event uses a source allowed by the regulatory body and is kept reasonably accurate and updated. As required by the regulatory body, controls shall be implemented for the operator to:

a) Review the accuracy and timeliness of any statistics/line services; and
b) When an incident or error occurs that results in a loss of communication with statistics/line services, record the incident or error in a log along with the date and time of occurrence, its duration, nature, and a description of its impact on the system's performance. This information shall be maintained for a period of 90 days, or as otherwise specified by the regulatory body.

### A.6.3 Suspending Markets or Events

There shall be established procedures for suspending markets or events (i.e. stop accepting wagers for that market or markets associated with that event). When wagering is suspended for an active event, an entry shall be made in an audit log that includes the date and time of suspension and its reason.

### A.6.4 Wager Cancellations

Wagering transactions cannot be modified except to be voided or cancelled as provided for in the operator's published cancellation policy. A cancellation grace period may be offered to allow players to request a cancellation of wagers placed. The following requirements apply to wager cancellations:

a) Player initiated cancellations may be authorized in accordance with the cancellation policy.
b) Operator initiated cancellations shall provide a reason for cancellation to a player (e.g., past-post wager).
c) An operator shall not void or cancel any wager without the prior approval of the regulatory body.

### A.6.5 Wagering Periods

Documentation shall be in place to provide how the wagering period is controlled. This would include any cases where the wagering period is first opened, when it is closed, or any other time in between where a wager is unable to be placed (e.g., odds/payouts and prices are being updated).

### A.6.6 Results

Before publicly announcing results and declaring winners, there shall be a policy for the confirmation of results based on qualified and approved sources, unless automated by an external feed. If an external feed is in use, there shall be procedures in place for cases where access to the external feed is unavailable. There shall also be a procedure in place to handle changes in results (e.g., due to statistics/line corrections).

### A.6.7 Winning Wager Payment

In the event of a failure of the Event Wagering System's ability to pay winning wagers, the operator shall have controls detailing the method of paying these wagers.

### A.6.8 Virtual Events

An operator who offers virtual event wagering shall maintain all information necessary to adequately reconstruct the virtual events, including the virtual event outcome and/or virtual participant actions, conducted within the past 90 days or as required by the regulatory body. This information may be recorded by the Event Wagering System or associated equipment, using some combination of text, logs, video, graphics, screen captures, or other means (e.g., "flight recorder" mechanism). Alternatively, procedures may be included to have the public display of the virtual event be recorded by the surveillance system.

## A.7 Wagering Venue Specifications

### A.7.1 Venue Verification Audit

The wagering venue will be required to meet the applicable aspects of the appropriate policy and/or procedure documents as determined by the operator in consultation with the regulatory body. To maintain the integrity of wagering operations, venues may be subject to an additional verification audit as required by the regulatory body. The following specifications apply to venues:

### A.7.2 Wagering Equipment

The venue shall provide a secure location for the placement, operation, and usage of wagering equipment, including Wagering Devices, displays, and communications equipment. Security policies and procedures shall be in place and reviewed periodically to ensure that risks are identified, mitigated and underwritten by contingency plans. In addition:

a) Wagering equipment shall be installed according to a defined plan and records of all installed wagering equipment shall be maintained.
b) Wagering equipment shall be sited or protected to reduce the risks from:

i. Environmental threats and hazards;
ii. Opportunities for unauthorized access;
iii. Power failures; and
iv. Other disruptions caused by failures in supporting utilities.

c) Access to the wagering equipment by an employee shall be controlled by a secure logon procedure or other secure process approved by the regulatory body to ensure that only authorized employees are allowed access. It shall not be possible to modify the configuration settings of the wagering equipment without an authorized secure process.
d) A user session, where supported by wagering equipment, is initiated by the employee logging in to their user account using their secure username and password or an alternative means for the employee to provide identification information as allowed by the regulatory body.
   i. All available options presented to the employee shall be tied to their user account.
   ii. If the wagering equipment does not receive input from the employee within 5 minutes, or a period specified by the regulatory body, the user session shall time out or lock up, requiring the employee to re-establish their login in order to continue.
e) To ensure its continued availability and integrity, wagering equipment shall be correctly maintained, inspected and serviced at regular intervals to ensure that it is free from defects or mechanisms that could interfere with its operation.
f) Prior to disposal or re-use, wagering equipment containing storage media shall be checked to ensure that any licensed software, player account information, and other sensitive information has been removed or securely overwritten (i.e., not just deleted).

### A.7.3 Wagering Operations

The following procedures shall be in place for wagering operations within the venue:

a) Procedures to enable a suitable response to any security issue within the venue.
b) Procedures to prevent any person from tampering with or interfering with the operation of any wagering or wagering equipment;
c) Procedures to describe the operations and the servicing of POS Wagering Devices and Self-Service Wagering Devices, including the handling of error conditions and performing reconciliations;
d) Procedures to ensure accessibility requirements observed by the regulatory body are met for the installation of Self-Service Wagering Devices.
e) Procedures for wager transactions using a POS Wagering Device, including:
   i. Accepting wagers from players only during the wager period;
   ii. Notifying players if their wager attempt is rejected;
   iii. Requiring the recording of player data or player account registration if their wager exceeds a value specified by the regulatory body;
   iv. Providing notification of any odds/payouts or price changes which occur while attempting to process a wager;
   v. Providing a player access to a wager record once the wager is authorized;
f) Procedures for handling cancelled events and withdrawn selections for wagers with multiple events (e.g., parlays), including providing refunds to players who were not refunded automatically by the system (e.g., wagers placed anonymously); and
g) Procedures for redemption of winning wagers, including:

i. Scanning the barcode of a wager record (via a barcode reader or equivalent); or
ii. Manually inputting the wager identification number and performing a verification with the system.

### A.7.4 Surveillance and Recording

The venue will be required to install, maintain, and operate a surveillance system that has the capability to monitor and record continuous unobstructed views of all wagering and financial transactions as well as any dynamic displays of wagering information. Procedures shall be in place to ensure that the recording:

a) Covers the defined wagering areas with sufficient detail to identify any discrepancies;
b) Is captured in such a way that precludes interference or deletion;
c) Can be reviewed by the operator and/or regulatory body in the event of a player complaint/dispute; and
d) Is kept for at least 90 days or as required by the regulatory body.

## A.8 Monitoring Procedures

### A.8.1 Monitoring for Collusion and Fraud

The operator shall take measures designed to reduce the risk of collusion or fraud, including having procedures for:

a) Identifying and/or refusing to accept suspicious wagers which may indicate cheating, manipulation, interference with the regular conduct of an event, or violations of the integrity of any event on which wagers were made;
b) Reasonably detecting irregular patterns or series of wagers to prevent player collusion or the unauthorized use of artificial player software; and
c) Monitoring and detecting events and/or irregularities in volume or swings in odds/payouts and prices which could signal suspicious activities as well as all changes to odds/payouts and prices and/or suspensions throughout an event.

### A.8.2 Anti-Money Laundering (AML) Monitoring

The operator shall have AML procedures and policies put in place, as required by the regulatory body, to ensure that:

a) Employees are trained in AML, and this training is kept up to date;
b) Player accounts are monitored for opening and closing in short time frames and for deposits and withdrawals without associated wagering transactions; and
c) Aggregate transactions over a defined period may require further due diligence checks and may be reportable to the relevant organization if they exceed the threshold prescribed by the regulatory body.

### A.8.3 Location Service Provider Monitoring

The operator, who offers remote wagering, or a third-party location service provider authorized by the regulatory body shall, where required by the regulatory body:

a) Have procedures to maintain a real-time data feed of all location checks and an up-to-date list of potential location fraud risks (e.g., fake location apps, virtual machines, remote desktop programs, etc.);
b) Offer an alert system to identify unauthorized or improper access;
c) Allow periodic audits to assess and measure its continued ability to detect and mitigate existing and emerging location fraud risks;
d) Ensure the location detection service or application used for location detection:
    i. Utilizes closed-source databases (IP, proxy, VPN, etc.) that are frequently updated and periodically tested for accuracy and reliability; and
    ii. Undergoes frequent updates to maintain cutting-edge data collection, device compatibility, and fraud prevention capabilities against location fraud risks.

# Appendix B: Operational Audit for Technical Security Controls

## B.1 Introduction

### B.1.1 General Statement

This appendix sets forth technical security controls which will be reviewed in an operational audit as a part of the Event Wagering System evaluation, including, but not limited to, an information security system (ISS) assessment, review of the operational processes that are critical to compliance, penetration testing focused on the external and internal infrastructure as well as the applications transferring, storing and/or processing player data and/or sensitive information, and any other objectives established by the regulatory body. The security controls outlined in this appendix apply to the following critical components of the system:

a) Components which record, store, process, share, transmit or retrieve sensitive information (e.g., validation numbers, PINs, player data);
b) Components which generate, transmit, or process random numbers used to determine the outcome of virtual events (if applicable);
c) Components which store results or the current state of a player's wager;
d) Points of entry to and exit from the above components (other systems which are able to communicate directly with core critical systems); and
e) Communication networks which transmit sensitive information.

**NOTE:** It is also recognized that additional technical security controls which are not specifically included within this standard will be relevant and required for an operational audit as determined by the operator and/or regulatory body within their rules, regulations, and Minimum Internal Control Standards (MICS).

## B.2 System Operation & Security

### B.2.1 System Procedures

The operator shall be responsible for documenting and following the relevant Event Wagering System procedures. These procedures shall at least include the following as required by the regulatory body:

a) Procedures for monitoring the critical components and the transmission of data of the entire system, including communication, data packets, networks, as well as the components and data transmissions of any third-party services involved, with the objective of ensuring integrity, reliability and accessibility;
b) Procedures and security standards for the maintenance of all aspects of security of the system to ensure secure and reliable communications, including protection from hacking or tampering;
c) Procedures for defining, monitoring, documenting, and reporting, investigating, responding to, and resolving security incidents, including detected breaches and suspected or actual hacking or tampering with the system;

d) Procedure for monitoring and adjusting resource consumption and maintaining a log of the system performance, including a function to compile performance reports;
e) Procedures to investigate, document and resolve malfunctions, which address the following:
   i. Determination of the cause of the malfunction;
   ii. Review of relevant records, reports, logs, and surveillance records;
   iii. Repair or replacement of the critical component;
   iv. Verification of the integrity of the critical component before restoring it to operation;
   v. Filing an incident report with the regulatory body and documenting the date, time and reason for the malfunction along with the date and time the system is restored; and
   vi. Voiding or cancelling wagers and pays if a full recovery is not possible.

### B.2.2 Physical Location of Servers

The Event Wagering System server(s) shall be housed in one or more secure location(s) which may be located locally, within a single venue, or may be remotely located outside of the venue as allowed by the regulatory body. In addition, secure location(s) shall:

a) Have sufficient protection against alteration, tampering or unauthorized access;
b) Be equipped with a surveillance system that shall meet the procedures put in place by the regulatory body;
c) Be protected by security perimeters and appropriate entry controls to ensure that access is restricted to only authorized personnel and that any attempts at physical access are recorded in a secure log; and
d) Be equipped with controls to provide physical protection against damage from fire, flood, hurricane, earthquake and other forms of natural or manmade disaster.

### B.2.3 Logical Access Control

The Event Wagering System shall be logically secured against unauthorized access by authentication credentials allowed by the regulatory body, such as passwords, multi-factor authentication, digital certificates, PINs, biometrics, and other access methods (e.g., magnetic swipe, proximity cards, embedded chip cards).

a) Each user shall have their own individual authentication credential whose provision shall be controlled through a formal process.
b) Authentication credential records shall be maintained either manually or by systems that automatically record authentication changes and force authentication credential changes.
c) The storage of authentication credentials shall be secure. If any authentication credentials are hard coded on a component of the system, they shall be encrypted.
d) A fallback method for failed authentication (e.g., forgotten passwords) shall be at least as strong as the primary method.
e) Lost or compromised authentication credentials and authentication credentials of terminated users shall be deactivated, secured or destroyed as soon as reasonably possible.
f) The system shall have multiple security access levels to control and restrict different classes of access to the server, including viewing, changing or deleting critical files and directories.

Procedures shall be in place to assign, review, modify, and remove access rights and privileges to each user, including:
   i. Allowing the administration of user accounts to provide an adequate separation of duties;
   ii. Limiting the users who have the requisite permissions to adjust critical system parameters;
   iii. The enforcement of adequate authentication credential parameters such as minimum length, and expiration intervals; and

g) Procedures shall be in place to identify and flag suspect accounts where authentication credentials may have been stolen.
h) Any logical access attempts to the system applications or operating systems shall be recorded in a secure log.
i) The use of utility programs which can override application or operating system controls shall be restricted and tightly controlled.

**NOTE:** Where passwords are used as an authentication credential, it is recommended that they are changed at least once every 90 days, are at least 8 characters in length and contain a combination of at least two of the following criteria: upper case letters, lower case letters, numeric and/or special characters.

### B.2.4 User Authorization

The Event Wagering System shall implement the following user authorization requirements:

a) A secure and controlled mechanism shall be employed that can verify that the system component is being operated by an authorized user on demand and on a regular basis as required by the regulatory body.
b) The use of automated equipment identification to authenticate connections from specific locations and equipment shall be documented and shall be included in the review of access rights and privileges.
c) Any authorization information communicated by the system for identification purposes shall be obtained at the time of the request from the system and not be stored on the system component.
d) The system shall allow for system administrator notification and user lockout or audit trail entry, after a set number of unsuccessful authorization attempts.

### B.2.5 Server Programming

The Event Wagering System shall be sufficiently secure to prevent any user-initiated programming capabilities on the server that may result in modifications to the database. However, it is acceptable for network or system administrators to perform authorized network infrastructure maintenance or application troubleshooting with sufficient access rights. The server shall also be protected from the unauthorized execution of mobile code.

### B.2.6 Verification Procedures

There shall be procedures in place for verifying on demand that the critical control program components of the Event Wagering System in the production environment are identical to those approved by the regulatory body.

a) Signatures of the critical control program components shall be gathered from the production environment through a process to be approved by the regulatory body.
b) The process shall include one or more analytical steps to compare the current signatures of the critical control program components in the production environment with the signatures of the current approved versions of the critical control program components.
c) The output of the process shall be stored in an unalterable format, which detail the verification results for each critical control program authentication and:
    i. Be recorded in a system log or report which shall be retained for a period of 90 days or as otherwise specified by the regulatory body;
    ii. Be accessible by the regulatory body in a format which will permit analysis of the verification records by the regulatory body; and
    iii. Comprise part of the system records which shall be recovered in the event of a disaster or equipment or software failure.
d) Any failure of verification of any component of the system shall require a notification of the authentication failure being communicated to the operator and regulatory body as required.
e) There shall be a process in place for responding to authentication failures, including determining the cause of the failure and performing the associated corrections or reinstallations needed in a timely manner.

### B.2.7 Electronic Document Retention System

Reports required by this standard and the regulatory body may be stored in an electronic document retention system provided that the system:

a) Is properly configured to maintain the original version along with all subsequent versions reflecting all changes to the report;
b) Maintains a unique signature for each version of the report, including the original;
c) Retains and reports a complete log of changes to all reports including who (user identification) performed the changes and when (date and time);
d) Provides a method of complete indexing for easily locating and identifying the report including at least the following (which may be input by the user):
    i. Date and time report was generated;
    ii. Application or system generating the report;
    iii. Title and description of the report;
    iv. User identification of who is generating the report; and
    v. Any other information that may be useful in identifying the report and its purpose;
e) Is configured to limit access to modify or add reports to the system through logical security of specific user accounts;
f) Is configured to provide a complete audit trail of all administrative user account activity;
g) Is properly secured through use of logical security measures (user accounts with appropriate access, proper levels of event logging, and document the version control, etc.);
h) Is physically secured with all other critical components of the Event Wagering System; and
i) Is equipped to prevent disruption of report availability and loss of data through hardware and software redundancy best practices, and backup processes.

### B.2.8 Asset Management

All assets housing, processing or communicating sensitive information, including those comprising the operating environment of the Event Wagering System and/or its components, shall be accounted for and have a nominated owner.

a) An inventory shall be drawn up and maintained of all assets holding controlled items.
b) A procedure shall exist for adding new assets and removing assets from service.
c) A policy shall be included on the acceptable use of assets associated with the system and its operating environment.
d) Each asset shall have a designated "owner" responsible for:
   i. Ensuring that information and assets are appropriately classified in terms of their criticality, sensitivity, and value; and
   ii. Defining and periodically reviewing access restrictions and classifications.
e) A procedure shall exist to ensure that recorded accountability for assets is compared with actual assets at intervals required by the regulatory body and appropriate action is taken with respect to discrepancies.
f) Copy protection to prevent unauthorized duplication or modification of software may be implemented provided that:
   i. The method of copy protection is fully documented and provided to the independent test laboratory, to verify that the protection works as described; or
   ii. The program or component involved in enforcing the copy protection can be individually verified by the methodology approved by the regulatory body.

## B.3 Backup and Recovery

### B.3.1 Data Security

The Event Wagering System shall provide a logical means for securing the player data and wagering data, including accounting, reporting, significant event, or other sensitive information, against alteration, tampering, or unauthorized access.

a) Appropriate data handling methods shall be implemented, including validation of input and rejection of corrupt data.
b) The number of workstations where critical applications or associated databases may be accessed shall be limited.
c) Encryption or password protection or equivalent security shall be used for files and directories containing data. If encryption is not used, the operator shall restrict users from viewing the contents of such files and directories, which at a minimum shall provide for the segregation of system duties and responsibilities as well as the monitoring and recording of access by any person to such files and directories.
d) The normal operation of any equipment that holds data shall not have any options or mechanisms that may compromise the data.
e) No equipment may have a mechanism whereby an error will cause the data to automatically clear.

f) Any equipment that holds data in its memory shall not allow removal of the information unless it has first transferred that information to the database or other secured component(s) of the system.
g) Data shall be stored in areas of the server that are encrypted and secured from unauthorized access, both external and internal.
h) Production databases containing data shall reside on networks separated from the servers hosting any user interfaces.
i) Data shall be maintained at all times regardless of whether the server is being supplied with power.
j) Data shall be stored in such a way as to prevent the loss of the data when replacing parts or modules during normal maintenance.

### B.3.2 Data Alteration

The alteration of any accounting, reporting or significant event data shall not be permitted without supervised access controls. In the event any data is changed, the following information shall be documented or logged:

a) Unique ID number for the alteration;
b) Data element altered;
c) Data element value prior to alteration;
d) Data element value after alteration;
e) Time and date of alteration; and
f) Personnel that performed alteration (user identification).

### B.3.3 Backup Frequency

Backup scheme implementation shall occur at least once every day or as otherwise specified by the regulatory body, although all methods will be reviewed on a case-by-case basis.

### B.3.4 Storage Medium Backup

Audit logs, system databases, and any other pertinent player data and wagering data shall be stored using reasonable protection methods. The Event Wagering System shall be designed to protect the integrity of this data in the event of a failure. Redundant copies of this data shall be kept on the system with open support for backups and restoration, so that no single failure of any portion of the system would cause the loss or corruption of data.

a) The backup shall be contained on a non-volatile physical medium, or an equivalent architectural implementation, so that should the primary storage medium fail, the functions of the system and the process of auditing those functions can continue with no critical data loss.
b) Where the regulatory body allows for the use of cloud platforms, if the backup is stored in a cloud platform, another copy may be stored in a different cloud platform.
c) If hard disk drives are used as backup media, data integrity shall be assured in the event of a disk failure. Acceptable methods include, but are not limited to, multiple hard drives in an acceptable RAID configuration, or mirroring data over two or more hard drives.

d) Upon completion of the backup process, the backup media is immediately transferred to a location physically separate from the location housing the servers and data being backed up (for temporary and permanent storage).
   i. The storage location is secured to prevent unauthorized access and provides adequate protection to prevent the permanent loss of any data.
   ii. Backup data files and data recovery components shall be managed with at least the same level of security and access controls as the system.

**NOTE:** The distance between the two locations should be determined based on potential environmental threats and hazards, power failures, and other disruptions but should also consider the potential difficulty of data replication as well as being able to access the recovery site within a reasonable time (Recovery Time Objective).

### B.3.5 System Failure

The Event Wagering System shall have sufficient redundancy and modularity so that if any single component or part of a component fails, the functions of the system and the process of auditing those functions can continue with no critical data loss. When two or more components are linked:

a) The process of all wagering operations between the components shall not be adversely affected by restart or recovery of either component (e.g., transactions are not to be lost or duplicated because of recovery of one component or the other); and
b) Upon restart or recovery, the components shall immediately synchronize the status of all transactions, data, and configurations with one another.

### B.3.6 Accounting of Master Resets

The operator shall be able to identify and properly handle the situation where a master reset has occurred on any component which affects wagering operations.

### B.3.7 Recovery Requirements

In the event of a catastrophic failure when the Event Wagering System cannot be restarted in any other way, it shall be possible to restore the system from the last backup point and fully recover. The contents of that backup shall contain the following critical information including, but not limited to:

a) The recorded information specified under the section entitled “Information to be Maintained”;
b) Specific site or venue information such as configuration, security accounts, etc.;
c) Current system encryption keys; and
d) Any other system parameters, modifications, reconfiguration (including participating sites or venues), additions, merges, deletions, adjustments and parameter changes.

### B.3.8 Uninterruptible Power Supply (UPS) Support

All system components shall be provided with adequate primary power. Where the server is a stand-alone application, it shall have an Uninterruptible Power Supply (UPS) connected and shall have sufficient capacity to permit a graceful shut-down and that retains all player data and wagering data during a power loss. It is acceptable that the system may be a component of a network that is supported by a network-wide UPS provided that the server is included as a device protected by the UPS. There shall be a surge protection system in use if not incorporated into the UPS itself.

### B.3.9 Business Continuity and Disaster Recovery Plan

A business continuity and disaster recovery plan shall be in place to recover wagering operations if the Event Wagering System's production environment is rendered inoperable. The business continuity and disaster recovery plan shall:

a) Address the method of storing player data and wagering data to minimize loss. If asynchronous replication is used, the method for recovering data shall be described or the potential loss of data shall be documented;
b) Delineate the circumstances under which it will be invoked;
c) Address the establishment of a recovery site physically separated from the production site;
d) Contain recovery guides detailing the technical steps required to re-establish wagering functionality at the recovery site; and
e) Address the processes required to resume administrative operations of wagering activities after the activation of the recovered system for a range of scenarios appropriate for the operational context of the system.

## B.4 Communications

### B.4.1 General Statement

This section will discuss the various wired and wireless communication methods, including communications performed across the internet or a public or third-party network, as allowed by the regulatory body.

### B.4.2 Connectivity

Only authorized devices shall be permitted to establish communications between any system components. The Event Wagering System shall provide a method to:

a) Enroll and un-enroll system components;
b) Enable and disable specific system components;
c) Ensure that only enrolled and enabled system components, including Wagering Devices, participate in wagering operations; and
d) Ensure that the default condition for components shall be un-enrolled and disabled.

### B.4.3 Communication Protocol

Each component of the Event Wagering System shall function as indicated by a documented secure communication protocol.

a) All protocols shall use communication techniques that have proper error detection and recovery mechanisms, which are designed to prevent intrusion, interference, eavesdropping and tampering. Any alternative implementations will be reviewed on a case-by-case basis and approved by the regulatory body.
b) All data communications critical to wagering or player account management shall employ encryption and authentication.
c) Communication on the secure network shall only be possible between approved system components that have been enrolled and authenticated as valid on the network. No unauthorized communications to components and/or access points shall be allowed.

### B.4.4 Communications Over Internet/Public Networks

Communications between any system components, including Wagering Devices, which takes place over internet/public networks, shall be secure by a means approved by the regulatory body. Player data, sensitive information, wagers, results, financial information, and player transaction information shall always be encrypted over the internet/public network and protected from incomplete transmissions, misrouting, unauthorized message modification, disclosure, duplication or replay.

### B.4.5 Wireless Local Area Network (WLAN) Communications

Wireless Local Area Network (WLAN) communications, as allowed by the regulatory body, shall adhere to the applicable jurisdictional requirements specified for wireless devices and network security. In the absence of specific jurisdictional standards, the "Wireless Device Requirements" and "Wireless Network Security Requirements" of the *GLI-26 Standards for Wireless Systems* shall be used as applicable.

**NOTE:** It is imperative for operators to review and update internal control policies and procedures to ensure the network is secure and threats and vulnerabilities are addressed accordingly. Periodic inspection and verification of the integrity of the WLAN is recommended.

### B.4.6 Network Security Management

Networks shall be logically separated such that there should be no network traffic on a network link which cannot be serviced by hosts on that link. The following requirements apply:

a) All network management functions shall authenticate all users on the network and encrypt all network management communications.
b) The failure of any single item shall not result in a denial of service.
c) An Intrusion Detection System/Intrusion Prevention System (IDS/IPS) shall be installed on the network which can listen to both internal and external communications as well as detect or prevent:
    i. Distributed Denial of Service (DDOS) attacks;
    ii. Shellcode from traversing the network;

iii. Address Resolution Protocol (ARP) spoofing; and
iv. Other "Man-In-The-Middle" attack indicators and sever communications immediately if detected.

d) In addition to the requirements in (c), an IDS/IPS installed on a WLAN shall be able to:
   i. Scan the network for any unauthorized or rogue access points or devices connected to any access point on the network at least quarterly or as defined by the regulatory body;
   ii. Automatically disable any unauthorized or rogue devices connected to the system; and
   iii. Maintain a history log of all wireless access for at least the previous 90 days or as otherwise specified by the regulatory body. This log shall contain complete and comprehensive information about all wireless devices involved and shall be able to be reconciled with all other networking devices within the site or venue.
e) Network Communication Equipment (NCE) shall meet the following requirements:
   i. NCE shall be constructed in such a way as to be resistant to physical damage to the hardware or corruption of the contained firmware/software by normal usage.
   ii. NCE shall be physically secured from unauthorized access.
   iii. System communications via NCE shall be logically secured from unauthorized access.
   iv. NCE with limited onboard storage shall, if the audit log becomes full, disable all communication or offload logs to a dedicated log server.
f) All network hubs, services and connection ports shall be secured to prevent unauthorized access to the network. Unused services and non-essential ports shall be either physically blocked or software disabled whenever possible.
g) In virtualized environments, redundant server instances shall not run under the same hypervisor.
h) Stateless protocols, such as UDP (User Datagram Protocol), shall not be used for sensitive information without stateful transport. Note that although HTTP (Hypertext Transport Protocol) is technically stateless, if it runs on TCP (Transmission Control Protocol) which is stateful, this is allowed.
i) All changes to network infrastructure (e.g., network communication equipment configuration) shall be logged.
j) Virus scanners and/or detection programs shall be installed on all systems. These programs shall be updated regularly to scan for new strains of viruses.

## B.5 Third-Party Service Providers

### B.5.1 Third-Party Communications

Where communications with third-party service providers are implemented, such as player loyalty programs, financial services (banks, payment processors, etc.), location service providers, cloud service providers, statistics/line services, and identity verification services, the following requirements apply:

a) The Event Wagering System shall be capable of securely communicating with third-party service providers using encryption and strong authentication.
b) All login events involving third-party service providers shall be recorded to an audit file.
c) Communication with third-party service providers shall not interfere or degrade normal Event Wagering System functions.

i. Third-party service provider data shall not affect player communications.
ii. Connections to third-party service providers shall not use the same network infrastructure as player connections.
iii. Wagering shall be disabled on all network connections except for the player network;
iv. The system shall not route data packets from third-party service providers directly to the player network and vice-versa
v. The system shall not act as IP routers between player networks and third-party service providers.

d) All financial transactions shall be reconciled with financial institutions and payment processors daily or as otherwise specified by the regulatory body.

### B.5.2 Third-Party Services

The security roles and responsibilities of third-party service providers shall be defined and documented as required by the regulatory body. The operator shall have policies and procedures for managing them and monitoring their adherence to relevant security requirements:

a) Agreements with third-party service providers involving accessing, processing, communicating or managing the system and/or its components, or adding products or services to the system and/or its components shall cover all relevant security requirements.
b) The services, reports and records provided by the third-party service providers shall be monitored and reviewed annually or as required by the regulatory body.
c) Changes to the provision of third-party service providers, including maintaining and improving existing security policies, procedures and controls, shall be managed, taking account of the criticality of systems and processes involved and re-assessment of risks.
d) The access rights of third-party service providers to the system and/or its components shall be removed upon termination of their contract or agreement or adjusted upon change.

## B.6 Technical Controls

### B.6.1 Domain Name Service (DNS) Requirements

The following requirements apply to the servers used to resolve Domain Name Service (DNS) queries used in association with the Event Wagering System.

a) The operator shall utilize a secure primary DNS server and a secure secondary DNS server which are logically and physically separate from one another.
b) The primary DNS server shall be physically located in a secure data center or a virtualized host in an appropriately secured hypervisor or equivalent.
c) Logical and physical access to the DNS server(s) shall be restricted to authorized personnel.
d) Zone transfers to arbitrary hosts shall be disallowed.
e) A method to prevent cache poisoning, such as DNS Security Extensions (DNSSEC), is required.
f) Multi-factor authentication shall be in place.
g) Registry lock shall be in place, so any request to change DNS server(s) will need to be verified manually.

### B.6.2 Cryptographic Controls

A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

a) Any player data and/or sensitive information shall be encrypted if it traverses a network with a lower level of trust.
b) Data that is not required to be hidden but shall be authenticated shall use some form of message authentication technique.
c) Authentication shall use a security certificate from an approved organization.
d) The grade of encryption used shall be appropriate to the sensitivity of the data.
e) The use of encryption algorithms shall be reviewed periodically to verify that the current encryption algorithms are secure.
f) Changes to encryption algorithms to correct weaknesses shall be implemented as soon as practical. If no such changes are available, the algorithm shall be replaced.
g) Encryption keys shall be stored on a secure and redundant storage medium after being encrypted themselves through a different encryption method and/or by using a different encryption key.

### B.6.3 Encryption Key Management

The management of encryption keys shall follow defined processes established by the operator and/or regulatory body. These defined processes shall cover the following:

a) Obtaining or generating encryption keys and storing them;
b) Managing the expiry of encryption keys, where applicable;
c) Revoking encryption keys;
d) Securely changing the current encryption keyset; and
e) Recovering data encrypted with a revoked or expired encryption key for a defined period after the encryption key becomes invalid.

## B.7 Remote Access and Firewalls

### B.7.1 Remote Access Security

Remote access is defined as any access from outside the system or system network including any access from other networks within the same site or venue. Remote access shall only be allowed if authorized by the regulatory body and shall:

a) Be performed via a secured method;
b) Have the option to be disabled;
c) Accept only the remote connections permissible by the firewall application and system settings;
d) Be limited to only the application functions necessary for users to perform their job duties:
    i. No unauthorized remote user administration functionality (adding users, changing permissions, etc.) is permitted; and
    ii. Unauthorized access to the operating system or to any database other than information retrieval using existing functions is prohibited.

**NOTE:** Remote access security will be reviewed on a case-by-case basis, in conjunction with the implementation of the current technology and approval from the regulatory body.

### B.7.2 Remote Access Procedures and Guest Accounts

A procedure for strictly controlled remote access shall be established. It is acknowledged that the supplier may, as needed, access the system and its associated components remotely for product and user support or updates/upgrades, as permitted by the regulatory body and the operator. This remote access shall use specific guest accounts which are:

a) Continuously monitored by the operator;
b) Disabled when not in use; and
c) Restricted through logical security controls to access only the necessary application(s) and/or database(s) for the product and user support or providing updates/upgrades.

### B.7.3 Remote Access Activity Log

The remote access application shall maintain an activity log which updates automatically depicting all remote access information, to include:

a) Identification of user(s) who performed and/or authorized the remote access;
b) Remote IP Addresses, Port Numbers, Protocols, and where possible, MAC Addresses;
c) Time and date the connection was made and duration of connection; and
d) Activity while logged in, including the specific areas accessed and changes made.

### B.7.4 Firewalls

All communications, including remote access, shall pass through at least one approved application-level firewall. This includes connections to and from any non-system hosts used by the operator.

a) The firewall shall be located at the boundary of any two dissimilar security domains.
b) A device in the same broadcast domain as the system host shall not have a facility that allows an alternate network path to be established that bypasses the firewall.
c) Any alternate network path existing for redundancy purposes shall also pass through at least one application-level firewall.
d) Only firewall-related applications may reside on the firewall.
e) Only a limited number of user accounts may be present on the firewall (e.g., network or system administrators only).
f) The firewall shall reject all connections except those that have been specifically approved.
g) The firewall shall reject all connections from destinations which cannot reside on the network from which the message originated (e.g., RFC1918 addresses on the public side of an internet firewall).
h) The firewall shall only allow remote access over the most up to date encrypted protocols.

### B.7.5 Firewall Audit Logs

The firewall application shall maintain an audit log and shall disable all communications and generate an error if the audit log becomes full. The audit log shall contain:

a) All changes to configuration of the firewall;
b) All successful and unsuccessful connection attempts through the firewall; and
c) The source and destination IP Addresses, Port Numbers, Protocols, and where possible, MAC Addresses.

**NOTE:** A configurable parameter 'unsuccessful connection attempts' may be utilized to deny further connection requests should the predefined threshold be exceeded. The system administrator shall also be notified.

### B.7.6 Firewall Rules Review

If required by the regulatory body, the firewall rules shall be periodically reviewed to verify the operating condition of the firewall and the effectiveness of its security configuration and rule sets and shall be performed on all the perimeter firewalls and the internal firewalls.

## B.8 Change Management

### B.8.1 General Statement

A change management policy is selected by the regulatory body for handling updates to the Event Wagering System and its components based on the propensity for frequent system upgrades and chosen risk tolerance. For systems that require frequent updates, a risk-based change management program may be utilized to afford greater efficiency in deploying updates. Risk-based change management programs typically include a categorization of proposed changes based on regulatory impact and define associated certification procedures for each category. The independent test laboratory will evaluate the system and future modifications in accordance with the change management policy selected by the regulatory body.

### B.8.2 Program Change Control Procedures

Program change control procedures shall be adequate to ensure that only authorized versions of programs are implemented on the production environment. These change controls shall include:

a) An appropriate software version control or mechanism for all software components and source code;
b) Records kept of all new installations and/or modifications to the system, including:
   i. The date of the installation or modification;
   ii. Details of the reason or nature of the installation or change such as new software, server repair, significant configuration modifications;
   iii. A description of procedures required to bring the new or modified component into service (conversion or input of data, installation procedures, etc.);
   iv. The identity of the user(s) performing the installation or modification;

c) A strategy for reverting back to the last implementation (rollback plan) if the install is unsuccessful, including complete backups of previous versions of software and a test of the rollback plan prior to implementation to the production environment;
d) A policy addressing emergency change procedures;
e) Procedures for testing and migration of changes;
f) Segregation of duties between the developers, quality assurance team, the migration team and users; and
g) Procedures to ensure that technical and user documentation is updated as a result of a change.

### B.8.3 Software Development Life Cycle

The acquisition and development of new software shall follow defined processes established by the operator and/or regulatory body.

a) The production environment shall be logically and physically separated from the development and test environments. When cloud platforms are used, no direct connection may exist between the production environment and any other environment.
b) Development staff shall be precluded from having access to promote code changes into the production environment.
c) There shall be a documented method to verify that test software is not deployed to the production environment.
d) To prevent leakage of sensitive information, there shall be a documented method to ensure that raw production data is not used in testing.
e) All documentation relating to software and application development shall be available and retained for the duration of its lifecycle.

### B.8.4 Patches

All patches should be tested whenever possible on a development and test environment configured identically to the target production environment. Under circumstances where patch testing cannot be thoroughly conducted in time to meet the timelines for the severity level of the alert and if authorized by the regulatory body, then patch testing should be risk managed, either by isolating or removing the untested component from the network or applying the patch and testing after the fact.

## B.9 Periodic Security Testing

### B.9.1 Technical Security Testing

Periodic technical security tests on the production environment shall be performed as required by the regulatory body to guarantee that no vulnerabilities putting at risk the security and operation of the Event Wagering System exist. These tests shall consist of a method of evaluation of security by means of an attack simulation by a third-party following a known methodology, and the analysis of vulnerabilities will consist in the identification and passive quantification of the potential risks of the system. Unauthorized access attempts shall be carried out up to the highest level of access possible and shall be completed with and without available authentication credentials (white box/black box

type testing). These allow assessments to be made regarding operating systems and hardware configurations, including but not limited to:

a) UDP/TCP port scanning;
b) Stack fingerprinting and TCP sequence prediction to identify operating systems and services;
c) Public Service Banner grabbing;
d) Web scanning using HTTP and HTTPS vulnerability scanners; and
e) Scanning routers using BGP (Border Gateway Protocol), BGMP (Border Gateway Multicast Protocol) and SNMP (Simple Network Management Protocol).

### B.9.2 Vulnerability Assessment

The purpose of the vulnerability assessment is to identify vulnerabilities, which could be later exploited during penetration testing by making basic queries relating to services running on the systems concerned. The assessment shall include at least the following activities:

a) External Vulnerability Assessment – The targets are the network devices and servers which are accessible by a third-party (both a person or a company), by means of a public IP (publicly exposed), related to the system from which is possible to access sensitive information.
b) Internal Vulnerability Assessment – The targets are the internal facing servers (within the DMZ, or within the LAN if there is no DMZ) related to the system from which is possible to access sensitive information. Testing of each security domain on the internal network shall be undertaken separately.

### B.9.3 Penetration Testing

The purpose of the penetration testing is to exploit any weaknesses uncovered during the vulnerability assessment on any publicly exposed applications or systems hosting applications processing, transmitting and/or storing sensitive information. The penetration testing shall include at least the following activities:

a) Network Layer Penetration Test – The test mimics the actions of an actual attacker exploiting weaknesses in the network security examining systems for any weakness that could be used by an external attacker to disrupt the confidentiality, availability and/or integrity of the network.
b) Application Layer Penetration Test – The test uses tools to identify weaknesses in the applications with both authenticated and unauthenticated scans, analysis of the results to remove false positives, and manual testing to confirm the results from the tools and to identify the impact of the weaknesses.

### B.9.4 Information Security Management System (ISMS) Audit

The audit of the Information Security Management System (ISMS) is to be conducted, including all the locations where sensitive information are accessed, processed, transmitted and/or stored. The ISMS will be reviewed against common information security principles in relation to confidentiality, integrity and availability, such as the following sources or equivalent:

a) ISO/IEC 27001 Information Security Management Systems (ISMS);
b) Payment Card Industry Data Security Standards (PCI-DSS); and
c) World Lottery Association Security Control Standards (WLA-SCS).

### B.9.5 Cloud Service Audit

An operator making use of a cloud service provider (CSP), as allowed by the regulatory body, to store, transmit or process sensitive information shall undergo a specific audit as required by the regulatory body. The CSP will be reviewed against common information security principles in relation to the provision and use of cloud services, such as ISO/IEC 27017 and ISO/IEC 27018, or equivalent.

a) If sensitive information is stored, processed or transmitted in a cloud environment, the applicable requirements will apply to that environment, and will typically involve validation of both the CSP's infrastructure and the operator's usage of that environment.
b) The allocation of responsibility between the CSP and the operator for managing security controls does not exempt an operator from the responsibly of ensuring that sensitive information is properly secured according to the applicable requirements.
c) Clear policies and procedures shall be agreed between the CSP and the operator for all security requirements, and responsibilities for operation, management and reporting shall be clearly defined and understood for each applicable requirement.

# Glossary of Key Terms

**Access Control –** The process of granting or denying specific requests for obtaining and using sensitive information and related services specific to a system; and to enter specific physical facilities which houses critical network or system infrastructure.

**Algorithm –** A finite set of unambiguous instructions performed in a prescribed sequence to achieve a goal, especially a mathematical rule or procedure used to compute a desired result. Algorithms are the basis for most computer programming.

**ARP, *Address Resolution Protocol* –** The protocol used to translate IP addresses into MAC addresses to support communication on a wireless or wired local area network.

**Audit Trail –** A record showing who has accessed a system and what operations the user has performed during a given period.

**Authentication –** Verifying the identity of a user, process, software package, or device, often as a prerequisite to allowing access to resources in a system.

**Backup –** A copy of files and programs made to facilitate recovery if necessary.

**Barcode** – An optical machine-readable representation of data. An example is a barcode found on printed wager records.

**Barcode Reader** – A device that is capable of reading or interpreting a barcode. This may extend to some smartphones or other electronic devices that can execute an application to read a barcode.

**Biometrics –** A biological identification input, such as fingerprints or retina patterns.

**Bluetooth –** A low power, short-range wireless communications protocol utilized for the interconnection of cellular phones, computers, and other electronic devices, including Wagering Devices. Bluetooth connections typically operate over distances of 10 meters or less and rely upon short-wavelength radio waves to transmit data over the air.

**Cache Poisoning** – An attack where the attacker inserts corrupt data into the cache database of the Domain Name Service (DNS).

**Commission –** An amount retained and not distributed by the operator from the total amount wagered on an event.

**Contingency Plan –** Management policy and procedures designed to maintain or restore wagering operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

**Coupon** – A wagering instrument that is used primarily for promotional purposes and which can be redeemed for restricted or unrestricted credits.

**Critical Component –** Any sub-system for which failure or compromise can lead to loss of player entitlements, government revenue or unauthorized access to data used for generating reports for the regulatory body.

**Critical Control Program** – A software program that controls behaviors relative to any applicable technical standard and/or regulatory requirement.

**Cryptographic RNG** – A Random Number Generator (RNG) which is resistant to attack or compromise by an intelligent attacker with modern computational resources who has knowledge of the source code of the RNG and/or its algorithm. Cryptographic RNGs cannot be feasibly 'broken' to predict future values.

**Data Integrity –** The property that data is both accurate and consistent and has not been altered in an unauthorized manner in storage, during processing, and while in transit.

**DDOS, *Distributed Denial of Service* –** A type of attack where multiple compromised systems, usually infected with a destructive software program, are used to target a single system. Victims of a DDOS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.

**Dividend –** The amount corresponding to the winner of a pari-mutuel wager.

**DNS, *Domain Name Service*** – The globally distributed internet database which (amongst other things) maps machine names to IP numbers and vice-versa.

**Domain –** A group of computers and devices on a network that are administered as a unit with common rules and procedures.

**DRP, *Disaster Recovery Plan* –** A plan for processing critical applications and preventing loss of data in the event of a major hardware or software failure or destruction of facilities.

**Encryption –** The conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized people.

**Encryption Key –** A cryptographic key that has been encrypted in order to disguise the value of the underlying plaintext.

**Event –** Occurrence related to sports, competitions, matches, and other types of activities approved by the regulatory body on which wagers may be placed.

**Event Wagering –** The wagering on sports, competitions, matches, and other event types approved by the regulatory body where the player places wagers on markets within an event.

**Event Wagering System –** The hardware, software, firmware, communications technology, other equipment, as well as operator procedures implemented in order to allow player participation in wagering, and, if supported, the corresponding equipment related to the display of the wager

outcomes, and other similar information necessary to facilitate player participation. The system provides the player with the means to place and manage wagers. The system provides the operator with the means to review player accounts, if supported, suspend events, generate various wagering/financial transaction and account reports, input outcomes for events, and set any configurable parameters.

**External Wagering System** – System hardware and software separate from that which comprises the Event Wagering System, which may drive the features common to wager offerings, wager configurations, reporting, etc. The player initially communicates directly with the Event Wagering System which can be integrated with one or more External Wagering Systems.

**Firewall** – A component of a computer system or network that is designed to block unauthorized access or traffic while still permitting outward communication.

**Fixed Odds Wagers –** Wager types where the payout is to be fixed at the time the wager is placed. If the predictions are correct, the odds are first multiplied by each other and then by the amount of the wager.

**Free Play Mode** – A mode that allows a player to participate in wagering without placing any financial wager, principally for the purpose of learning or understanding wagering mechanics.

**Geolocation** – Identifying the real-world geographic location of an internet connected Remote Wagering Device.

**Group Membership** – A method of organizing user accounts into a single unit (by job position) whereby access to system functions may be modified at the unit level and the changes take effect for all user accounts assigned to the unit.

**Hash Algorithm –** A function that converts a data string into an alpha-numeric string output of fixed length.

**HTTP, *Hypertext Transfer Protocol*** – The underlying protocol used to define how messages are formatted and transmitted, and what actions servers and browsers shall take in response to various commands.

**In-Play Wager** – A wager that is placed while an event is in-progress or actually taking place.

**Information Security** – Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability

**Internet** – An interconnected system of networks that connects computers around the world via TCP/IP.

**IDS/IPS, *Intrusion Detection System/Intrusion Prevention System*** – A system that inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a

network or system attack from someone attempting to break into or compromise a system. Used in computer security, intrusion detection refers to the process of monitoring computer and network activities and analyzing those events to look for signs of intrusion in your system.

**IP Address, *Internet Protocol Address* –** A unique number for a computer that is used to determine where messages transmitted on the Internet should be delivered. The IP address is analogous to a house number for ordinary postal mail.

**Jailbreaking** – Modifying a smartphone or other electronic device to remove restrictions imposed by the manufacturer or operator to allow the installation of unauthorized software.

**Key –** A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification.

**Key Management** – Activities involving the handling of cryptographic keys and other related security parameters (e.g., passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.

**Line Posting** – A value that establishes a wager's potential payout (e.g., money line + 175) or the conditions for a wager to be considered a win or loss (e.g., point spread + 2.5).

**MAC, *Message Authentication Code* –** A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.

**Malware –** A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

**"Man-In-The-Middle" Attack** – An attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

**Market** – A wager type (e.g., money line, spread, over/under) on which opportunities are built for wagering on one or more events.

**Message Authentication –** A security measure designed to establish the authenticity of a message by means of an authenticator within the transmission derived from certain predetermined elements of the message itself.

**Mobile Code** – Executable code that moves from computer to computer, including both legitimate code and malicious code such as computer viruses.

**Multi-Factor Authentication** – A type of authentication which uses two or more of the following to verify a user's identity: Information known only to the user (e.g., a password, pattern or answers to challenge questions); An item possessed by a user (e.g., an electronic token, physical token or an identification card); A user's biometric data (e.g., fingerprints, facial or voice recognition).

**NCE, *Network Communication Equipment*** – One or more devices that controls data communication in a system including, but not limited to, cables, switches, hubs, routers, wireless access points, and telephones

**Operator –** A person or entity that operates an Event Wagering System, using both the technological capabilities of the Event Wagering System as well as their own internal procedures.

**Pari-Mutuel Wagers –** Wager types where individual wagers are gathered into a pool. The winnings are calculated by sharing the pool among all winning bets.

**Parlay** – A single wager that links together two or more individual wagers and is dependent on all of those wagers winning together.

**Participant** – The athlete, team, or other entity that competes in an event.

**Password –** A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

**Past-Post Wager** – A wager that was made after the result of an event is accepted or after the selected participant has gained a material advantage (e.g., a score).

**Perfecta** (aka "Exacta") – A wager in which the player picks the first and second place finishers in a competition in the correct order.

**Physics Engine –** Specialized software that approximates the laws of physics, including behaviors such as motion, gravity, speed, acceleration, mass, etc. for a virtual event's elements or objects. The physics engine is utilized to place virtual event elements/objects into the context of the physical world when rendering computer graphics or video simulations.

**PIN, *Personal Identification Number* –** A numerical code associated with an individual and which allows secure access to a domain, account, network, system, etc.

**Player Account** (aka "Wagering Account") **–** An account maintained for a player where information relative to wagering and financial transactions are recorded on behalf of the player including, but not limited to, deposits, withdrawals, wagers, winnings, and balance adjustments. The term does not include an account used solely by an operator to track promotional points or credits or similar benefits issued by an operator to a player which may be redeemed for merchandise and/or services.

**Player Data** – Sensitive information regarding a player and which may include items such as full name, date of birth, place of birth, social security number, address, phone number, medical or employment history, or other personal information as defined by the regulatory body.

**Player Loyalty Program –** A program that provides incentives for players based on the volume of play or revenue received from a player.

**POS Wagering Device, *Point-of-Sale Wagering Device* –** An attendant station that at a minimum will be used by an attendant for the execution or formalization of wagers placed on behalf of a player.

**Port –** A physical entry or exit point of a module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire).

**Printer –** A Wagering Device peripheral that prints wager records and/or wagering instruments.

**Proxy –** A proxy is an application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. This effectively closes the straight path between the internal and external networks. Making it more difficult for an attacker to obtain internal addresses and other details of the internal network.

**Protocol –** A set of rules and conventions that specifies information exchange between devices, through a network or other media.

**Quinella** – A wager in which the first two places in a competition shall be predicted, but not necessarily in the finishing order.

**Remote Access –** Any access from outside the system or system network including any access from other networks within the same site or venue.

**Remote Wagering –** Wagering conducted using Remote Wagering Devices on an in-venue wireless network or over the internet, depending on the implementation(s) authorized by the regulatory body.

**Remote Wagering Device –** A player-owned device operated either on an in-venue wireless network or over the internet that at a minimum will be used for the execution or formalization of wagers placed by a player directly. Examples of a Remote Wagering Device include a personal computer, mobile phone, tablet, etc.

**Risk –** The likelihood of a threat being successful in its attack against a network or system.

**RNG, *Random Number Generator* –** A computational or physical device, algorithm, or system designed to produce numbers in a manner indistinguishable from random selection.

**Rooting** – Attaining root access to the operating system code to modify the software code on the mobile phone or other Remote Wagering Device or install software that the manufacturer would not allow to be installed.

**Secure Communication Protocol** – A communication protocol that provides the appropriate confidentiality, authentication and content integrity protection.

**Security Certificate** – Information, often stored as a text file that is used by the TSL (Transport Socket Layers) Protocol to establish a secure connection. A Security Certificate contains information

about whom it belongs to, who it was issued by, valid dates, a unique serial number or other unique identification that can be used to verify the contents of the certificate. In order for an TSL connection to be created, both sides shall have a valid Security Certificate, which is also called a Digital ID.

**Security Policy** – A document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance

**Self-Service Wagering Device –** A kiosk that at a minimum will be used for the execution or formalization of wagers placed by a player directly and, if supported, may be used for redemption of winning wager records.

**Sensitive Information** – Information such as player data, wagering data, validation numbers, PINs, passwords, secure seeds and keys, and other data that shall be handled in a secure manner.

**Server –** A running instance of software that is capable of accepting requests from clients, and the computer that executes such software. Servers operate within a Client-Server Architecture, in which "servers" are computer programs running to serve the requests of other programs ("clients"). In this case the "server" would be the Event Wagering System and the "clients" would be the Wagering Devices.

**Shellcode –** A small piece of code used as a payload in the exploitation of security. Shellcode exploits vulnerability and allows an attacker the ability to reduce a system's information assurance.

**Stateless Protocol –** A communications scheme that treats each request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of requests and responses.

**System Administrator –** The individual(s) responsible for maintaining the stable operation of the Event Wagering System (including software and hardware infrastructure and application software).

**TCP/IP, *Transmission Control Protocol/Internet Protocol* –** The suite of communications protocols used to connect hosts on the Internet.

**Threat –** Any circumstance or event with the potential to adversely impact network operations (including mission, functions, image, or reputation), assets, or individuals through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a system vulnerability.

**Time Stamp –** A record of the current value of the Event Wagering System date and time which is added to a message at the time the message is created.

**Touch Screen** – A video display device that also acts as a user input device by using electrical touch point locations on the display screen.

**Trifecta** – A wager in which a player wins by selecting the first three finishers of a competition in the correct order of finish.

**Unauthorized Access** – A person gains logical or physical access without permission to a network, system, application, data, or other resource.

**User Interface** – An interface application or program through which the user views and/or interacts with the Wagering Software to communicate their actions to the Event Wagering System.

**Version Control –** The method by which an evolving approved Event Wagering System is verified to be operating in an approved state.

**Virtual Event Wagering** – A form of wagering that allows for the placement of wagers on sports, contests, and matches whose results are determined solely by an approved Random Number Generator (RNG).

**Virtual Participant** – The athlete or other entity that competes in a virtual event.

**Virus** – A self-replicating program, typically with malicious intent, that runs and spreads by modifying other programs or files.

**Virus Scanner –** Software used to prevent, detect and remove computer viruses, including malware, worms and Trojan horses.

**Voucher –** A wagering instrument which can be redeemed for cash or used to subsequently redeem for credits.

**VPN, *Virtual Private Network* –** A logical network that is established over an existing physical network and which typically does not include every node present on the physical network.

**Vulnerability –** Software, hardware, or other weaknesses in a network or system that can provide a "door" to introducing a threat.

**Wager –** Any commitment of credits or money by the player on the results of events.

**Wager Record –** A printed ticket or electronic message confirming the acceptance of one or more wagers.

**Wagering Device –** An electronic device that converts communications from the Event Wagering System into a human interpretable form and converts human decisions into communication format understood by the Event Wagering System.

**Wagering Instrument –** A printed or virtual representative of value, other than a chip or token and includes coupons and vouchers. A virtual wagering instrument is an electronic token exchanged between a player's mobile device and the wagering device which is used for credit insertion and redemption.

**Wagering Rules –** Any written, graphical, and auditory information provided to the public regarding event wagering operations.

**Wagering Software** – The software used to take part in wagering and financial transactions with the Event Wagering System which, based on design, is downloaded to or installed on the Wagering Device, run from the Event Wagering System which is accessed by the Wagering Device, or a combination of the two. Examples of Wagering Software include proprietary download software packages, html, flash, etc.

**Wi-Fi –** The standard wireless local area network (WLAN) technology for connecting computers and electronic devices to each other and/or to the internet.

# Table of Contents

~~***2.17.6 Printer Location***. If a gaming device is equipped with a printer, it shall be located within a secure area of the gaming device, but not be housed within the logic area or the drop box.~~

~~***2.17.7 Printer Error Conditions***. A gaming device that is equipped with a printer shall have mechanisms to allow critical control program software to interpret and act upon the conditions listed below. If a printer error condition is identified, the gaming device shall display an appropriate error message and sound an alarm and/or illuminate the tower light. The error condition shall be communicated to the on-line system, when such a compatible system and protocol is supported. Additionally, for the conditions stated immediately below in (b), the printer shall be disabled. Printer error conditions shall include:~~

~~a) Out of paper/paper low; it is permissible for the gaming device to not lock up for these conditions, however, there shall be a means for the attendant to be alerted;~~
~~b) Printer jam/failure;~~
~~c) Printer disconnected; it is permissible for the gaming device to detect this error condition when the game tries to print; and~~
~~d) Once a printer error condition has been cleared, any unprinted voucher shall be generated or a suitable handpay shall be processed.~~

## 2.18 Machine Vouchers

***2.18.1 Payment by Voucher***. Payment by voucher as a method of credit redemption is only permissible when:

a) The gaming device is linked to a computerized validation system which allows for the validation of the voucher. Provisions must be made if communication is lost and validation information cannot be sent to the validation system, thereby requiring the manufacturer to support some alternate method of payment; or
b) Utilizing an approved alternative method that includes the ability to identify duplicate vouchers to prevent fraud through the redemption of a voucher that was previously issued by the gaming device.

***2.18.2 Voucher Information.*** A voucher shall contain the following information at a minimum:

a) Casino name / site identification (for a printed paper voucher, it is permissible for this information to be contained on the ticket stock itself);
b) Machine identification number;
c) Date and time;
d) Alpha value of the voucher in local monetary units;
e) Numeric value of the voucher in local monetary units;
f) Voucher sequence number;
g) Validation number (and which for a printed paper voucher, must appear on the leading edge of the ticket);
h) Bar code or any machine readable code representing the validation number;
i) Indication if the voucher is a "duplicate", assuming duplicate vouchers may be printed by the gaming device;
j) Type of transaction or other method of differentiating voucher types (assuming multiple voucher types are available). Additionally, it is strongly recommended that whenever the voucher type is itself a non-cashable item and/or just a receipt, that the voucher explicitly states that it has "no cash value" or other equivalent wording; and
k) Indication of an expiration period from date of issue, or date the voucher will expire (for a printed paper voucher, it is permissible for this information to be contained on the ticket stock itself).

*NOTE: Some of the above-listed information may also be part of the validation number or barcode. Multiple barcodes are allowed and may represent more than just the validation number.*

***2.18.3 Voucher-Out Log.*** The gaming device shall have the ability to retain information on the last twenty-five (25) issued vouchers in a voucher-out log. The voucher-out log shall contain the following information for each recorded voucher:

a) Value of credits in local monetary units in numerical form;

b) Time of day the voucher was issued, in twenty-four (24) hour format showing hours and minutes;
c) Date, in any recognized format, indicating the day, month, and year; and
d) Validation number. The gaming device shall mask all but the last 4 digits of the validation number as displayed in the twenty-five (25) voucher-out log.

***2.18.4 Online Voucher Issuance***. The gaming device may pay the player by issuing a printed or virtual voucher that contains the information as indicated in the section entitled "Voucher Information" above. Additionally, the gaming device shall support the transmission of the following information to the ticketing system regarding each voucher issued, as required by the communications protocol supported:

a) Value of credits in local monetary units in numerical form;
b) Time of day the voucher was printed in twenty-four (24) hour format showing hours and minutes;
c) Date, in any recognized format, indicating the day, month, and year;
d) Gaming device asset number; and
e) Validation number.

***2.18.5 Offline Voucher Issuance***. The gaming device shall meet the following minimum set of requirements to support the issuance of offline vouchers after a loss of communication with the validation system has been identified:

a) The gaming device shall not issue more offline vouchers than it has the ability to retain and display in the voucher out log;
b) The gaming device shall not request validation numbers, or values for seeds, keys, etc. used in the issuance of vouchers, until all outstanding offline voucher information has been fully communicated to the voucher validation system;
c) The gaming device shall request a new set of validation numbers, seeds, keys, etc. if the current list has the possibility of being compromised;
d) The values for the seeds, keys, etc. shall never be viewable through any display supported by the gaming device; and

e) An "offline authentication identifier" shall be included on the voucher. For printed paper vouchers, this identifier must appear on the next line immediately following the leading edge validation number that in no way overwrites, or otherwise compromises, the printing of the validation number on the voucher (not required for vouchers that are non-redeemable at a gaming device). The offline authentication identifier must be derived by a hash, or other secure encryption method of at least 128 bits, that will uniquely identify the voucher, verify that the redeeming system was also the issuing system, and validate the amount of the voucher. For cases where a suitable authentication identifier is not included on the voucher, the gaming device must issue at most one voucher after the communications between the gaming device and the system have been lost.

***2.18.6 Online Voucher Redemption***. Vouchers may be accepted by a gaming device connected to a ticket validation system provided that no credits are issued to the gaming device prior to confirmation of voucher validity.

## ~~2.19 Machine Communication Protocol~~

~~***2.19.1 Integrity of Protocol Communications***. For gaming devices that are designed to support communications with an on-line system, the device shall accurately function as indicated by the communications protocol that is implemented, and as required by the regulatory body, including, but not limited to, protocol-based metering and remote verification of the critical control program, where supported. In addition, the following rules shall be met:~~

~~a) With the exception of 'disable' commands, communications shall not negatively impact player interaction on the gaming device, including a player's access to all screen displays; and~~

~~b) After a program interruption, any communications to an external device shall not begin until the program resumption routine, including any self-test, is completed successfully.~~

# Table of Contents

# Chapter 4: Validation System Requirements

## 4.1 Introduction

### 4.1.1 General Statement

A Validation System may be entirely integrated into another system or exist as an entirely separate Gaming System. Validation Systems are generally classified into two types:

a) Bi-directional Validation Systems that allow Gaming Equipment to issue and redeem wagering instruments (TITO); and
b) Single-directional Validation Systems that allow Gaming Equipment to issue wagering instruments but do not allow Gaming Equipment to redeem wagering instruments.

**NOTE:** This chapter primarily addresses bi-directional Validation Systems. Where single-directional Validation Systems are utilized, some of this chapter may not apply.

## 4.2 Wagering Instruments

### 4.2.1 Wagering Instrument Communications

The Validation System shall process wagering instrument transactions correctly according to the secure communication protocol implemented.

### 4.2.2 Wagering Instrument Information

A wagering instrument shall contain the following information at a minimum:

a) The date and time of issuance;
b) Numeric value of the wagering instrument;
c) Unique validation number, and which for a printed wagering instrument, shall appear on the leading edge of the wagering instrument;
d) Barcode representing the unique validation number;
e) Unique Gaming Equipment ID or equivalent which issued the wagering instrument;
f) The type of wagering instrument or other method of differentiating wagering instrument types, assuming multiple types are available. Additionally, it is strongly recommended that whenever the wagering instrument type is itself a non-cashable coupon and/or just a receipt, that the wagering instrument explicitly states that it has “no cash value” or other equivalent wording;
g) For a printed wagering instrument, it is permissible for the following information to be contained on the ticket stock itself:
    i. Gaming Venue Name/Site Identifier; and
    ii. Indication of an expiration period from date of issue, or date the wagering instrument will expire;
    i. Indication if the wagering instrument is a “duplicate”, assuming duplicate wagering instruments may be printed;
h) For a printed wagering instrument which can be redeemed without attendant intervention, the following additional information shall also be printed:
    i. Alpha value of the wagering instrument; and

ii. Wagering instrument sequence number, which may be preprinted or concurrently-printed.

**NOTE:** Some of the above-listed information may also be part of the validation number or barcode. Multiple barcodes are allowed and may represent more than just the validation number.

### 4.2.3 Wagering Instrument Records

For each wagering instrument, the Validation System shall maintain the following information in a database, as applicable:

a) Unique validation number;
b) The date and time of issuance;
c) Value of the wagering instrument;
d) Unique Gaming Equipment ID or equivalent which issued the wagering instrument;
e) For Multi-Venue Validation Systems, Gaming Venue Name/Site Identifier where issuance occurred;
f) The type of wagering instrument or other method of differentiating wagering instrument types, assuming multiple types are available;
g) Indication of an expiration period from date of issue, or date the wagering instrument will expire;
h) For a redeemed wagering instrument (blank until known):
   i. The date and time of redemption;
   ii. Unique Gaming Equipment ID or equivalent which redeemed the wagering instrument;
   iii. For Multi-Venue Validation Systems, Gaming Venue Name/Site Identifier where redemption occurred;
i) For a voided wagering instrument (blank until known):
   i. The date and time of voiding;
   ii. Unique Gaming Equipment ID or equivalent which voided the wagering instrument;
   iii. For Multi-Venue Validation Systems, Gaming Venue Name/Site Identifier where voiding occurred;
j) For an expired wagering instrument, the date and time of expiration (blank until known); and
k) The current status of the wagering instrument (i.e., valid, unredeemed, pending, void, invalid, redemption in progress, redeemed, expired, etc.).

## 4.3 Wagering Instrument Issuance

### 4.3.1 Wagering Instrument Issuance

The Gaming Equipment may pay the player by issuing a printed or virtual wagering instrument that contains the information as indicated in the section entitled “Wagering Instrument Information” above. Payment by wagering instrument is only permissible when:

a) The Gaming Equipment is linked to a Validation System which allows for the validation of the wagering instrument. Provisions shall be made if communication is lost and validation information cannot be sent to the Validation System, thereby requiring the manufacturer to support some alternate method of payment; or
b) Utilizing an approved alternative method that includes the ability to identify duplicate wagering instruments to prevent fraud through the redemption of a wagering instrument that was previously issued by the Gaming Equipment.

### 4.3.2 Wagering Instrument Issuance Limits

Payment by wagering instruments where the amounts being paid exceed a Gaming Equipment or system configured limit (i.e., the credit limit, transaction limit, etc.) shall result in a handpay lockup or tilt on the Gaming Equipment.

### 4.3.3 Online Wagering Instrument Issuance

The Validation System and Gaming Equipment shall support the bi-directional transmission of the following information when issuing a wagering instrument, as applicable:

a) The date and time of issuance;
b) Value of the wagering instrument;
c) Unique validation number;
d) Unique Gaming Equipment ID or equivalent which issued the wagering instrument;
e) Gaming Venue Name/Site Identifier; and
f) Indication of an expiration period from date of issue, or date the wagering instrument will expire.

### 4.3.4 Validation Number Generation

The wagering instrument's unique validation number shall be generated by the Validation System or the Gaming Equipment:

a) Where the unique validation number is generated by the Gaming Equipment, the Validation System shall send a unique seed to the Gaming Equipment upon enrolling the Gaming Equipment as wagering instrument capable. The Validation System may subsequently send a new seed to the Gaming Equipment after a wagering instrument is issued.
b) The algorithm or method used to generate the unique validation number and determine the seed shall guarantee the unlikelihood of repetitive validation numbers.

### 4.3.5 Wagering Instrument Issuance During Communication Loss

Unless the Validation System and Gaming Equipment support offline wagering instrument issuance, the following requirements shall be met:

a) When using a non-seeded method, if any links between the Gaming Equipment and the Validation System go down, the Gaming Equipment shall:
    i. Not respond to the validation request and stop wagering instrument issuance;
    ii. Prevent further issuance of wagering instruments; or
    iii. Not read or store any further wagering instrument information generated by the Gaming Equipment.
b) In cases where the Gaming Equipment has already been 'seeded' by the Validation System, a maximum of two wagering instruments directly after loss of communication is acceptable, provided the wagering instrument issuance information is sent immediately, when communication is reestablished.

### 4.3.6 Offline Wagering Instrument Issuance

For the support of offline wagering instrument issuance, the Gaming Equipment shall be linked to an approved Validation System that allows validation of the wagering instrument but does not have to be in constant communication for the issuance of wagering instrument to be permissible. The following requirements shall be met to support the issuance of offline wagering instruments after a loss of communication with the Validation System has been identified:

a) The Gaming Equipment shall not issue more offline wagering instruments than it has the ability to store locally.
b) The Gaming Equipment shall not request validation numbers, or values for seeds, keys, etc. used in the issuance of wagering instruments, until all outstanding offline wagering instrument information has been fully communicated to the Validation System.
c) The Gaming Equipment shall request a new set of validation numbers, seeds, keys, etc. if the current list has the possibility of being compromised.
d) The complete validation numbers, or values for the seeds, keys, etc. shall never be viewable through any display mechanism supported by the Gaming Equipment.
e) The Validation System shall be able to set an expiration length for all provided and still unused validation numbers and seed, key, etc. values. Expired validation numbers and seed, key, etc. values shall be discarded in a way that prevents the re-use of unique combinations of validation numbers and seed, key, etc. values for a sufficient period of time on the system.
    i. Secure seeds, keys, etc. as assigned shall be sufficiently random. Measures to avoid predictability will be reviewed by the independent test laboratory on a case-by-case basis.
    ii. The minimum length for any secure seeds, keys, etc. employed by the Validation System shall be chosen from a pool of the variable type specified by the communication protocol utilized. The pool shall be comprised of at least 10 to the power of 14 randomly distributed values.
f) An “offline authentication identifier” shall be included on the wagering instrument.
    i. For printed wagering instruments, this identifier shall appear on the next line immediately following the leading-edge validation number that in no way overwrites, or otherwise compromises, the printing of the validation number on the wagering instrument (not required for wagering instruments that are non-redeemable without attendant intervention).
    ii. For cases where a suitable authentication identifier is not included on the wagering instrument, the Gaming Equipment shall issue at most one wagering instrument after the communications between the Gaming Equipment and the system have been lost.
g) The offline authentication identifier shall be derived by a hash algorithm, or other secure cryptographic method of at least 128 bits, that will uniquely identify the wagering instrument, verify that the redeeming system was also the issuing system, and validate the amount of the wagering instrument. The following minimum set of inputs shall be used to create the offline authentication identifier:
    i. Unique Gaming Equipment ID or equivalent;
    ii. Unique validation number;
    iii. Value of the wagering instrument; and
    iv. Secure seed, key, etc. provided by the Validation System to the Gaming Equipment.

## 4.4 Wagering Instrument Redemption

### 4.4.1 Wagering Instrument Redemption Process

The Validation System shall update the wagering instrument status on the database during each phase of the redemption process accordingly. In other words, whenever the wagering instrument status changes, the system shall update the database. Upon each status change, the database shall indicate the following information:

a) Unique validation number;
b) Value of the wagering instrument;
c) The date and time of status change; and
d) The current status of the wagering instrument (i.e., valid, unredeemed, pending, void, invalid, redemption in progress, redeemed, etc.).

### 4.4.2 Wagering Instrument Redemption Limits

If a player redeems a wagering instrument and that redemption would exceed Gaming Equipment or system configured limits (i.e., the credit limit, transaction limit, etc.) then this wagering instrument may only be redeemed provided that the player is clearly notified that they have redeemed less than requested to avoid player disputes, and the Gaming Equipment issues a wagering instrument that reflects the remaining credits.

### 4.4.3 Online Wagering Instrument Redemption

Wagering instruments can be redeemed at any Gaming Equipment which is enrolled for wagering instrument validation with a Validation System provided that no credits are issued to the Gaming Equipment prior to confirmation of wagering instrument validity.

### 4.4.4 Offline Wagering Instrument Redemption

If supported, offline wagering instruments can be redeemed at Cashier Station provided they are enrolled for wagering instrument validation with a Validation System and the identification and redemption of offline wagering instruments are supported through a system provided application.

## 4.5 Cashier Station Operation

### 4.5.1 Cashier Wagering Instrument Redemption

When wagering instruments are presented for redemption at a Cashier Station, the cashier shall scan the barcode (via a barcode reader or equivalent) or manually input the validation number and perform a verification with the Validation System.

### 4.5.2 Invalid Wagering Instrument Notification

The Validation System shall have the ability to identify and provide a notification to the Cashier Station in the case of invalid or unredeemable wagering instrument for the following conditions:

a) Wagering instrument cannot be found on file or has expired;
b) Wagering instrument has already been paid or voided; or
c) The value of wagering instrument differs from amount on file. This requirement can be met by display of wagering instrument for confirmation by the Cashier Station during the redemption process.

### 4.5.3 Wagering Instrument Redemption Receipt

The Cashier Station may issue a redemption receipt, after the wagering instrument is electronically validated, if applicable. If printed, the redemption receipt, at a minimum, shall contain the following information:

a) Unique Gaming Equipment ID or equivalent which issued the wagering instrument;
b) Unique validation number;
c) The date and time of redemption;
d) Value of the wagering instrument; and
e) Unique Cashier Station ID or user account ID which redeemed the wagering instrument.

## 4.6 Wagering Instrument Meters and Logs

### 4.6.1 Information Access

The wagering instrument meters and transaction logs required by this section shall have the ability to be displayed on demand using an authorized access method to ensure that only authorized personnel are allowed access. The meters and logs may be maintained locally by the Gaming Equipment and/or by an external critical component which records these meters and logs.

### 4.6.2 Wagering Instrument Meters

Electronic accounting meters shall be at least ten digits in length. Eight digits shall be used for the integer currency (e.g., dollar) amount and two digits used for the sub-currency (e.g., cents) amount. The meters shall automatically roll over to zero once its maximum logical value has been reached. Meters shall be labeled so they can be clearly understood in accordance with their function.

a) The required electronic accounting meters for each Gaming Equipment are as follows:
   i. Voucher In. There shall be a meter that accumulates the total value of all wagering vouchers accepted by the Gaming Equipment;
   ii. Voucher Out. There shall be a meter that accumulates the total value of all wagering vouchers issued by the Gaming Equipment;
   iii. Coupon Promotion In. There shall be a meter that accumulates the total value of all promotional coupons accepted by the Gaming Equipment;
   iv. Coupon Promotion Out. There shall be a meter that accumulates the total value of all promotional coupons issued by the Gaming Equipment; and
   v. Other Meters. Wagering instrument transactions that would not otherwise be metered under any of the above meters, shall be recorded on sufficient meters to properly reconcile all such transactions.

b) The operation of other mandatory meters for Gaming Equipment shall not be impacted directly by wagering instrument transactions.

**NOTE:** Any accounting meter that is not supported by the functionality of the Gaming Equipment is not required to be implemented by the supplier.

### 4.6.3 Wagering Instrument Transaction Log

There shall be the capacity to display a complete transaction log for the previous thirty-five transactions that incremented any of the "Wagering Instrument Meters". The following information shall be displayed:

a) The type of transaction (e.g., wagering instrument issuance/redemption, etc.);
b) The type of wagering instrument or other method of differentiating wagering instrument types, assuming multiple types are available;
c) The transaction value in local monetary units in numerical form;
d) The time of day of the transaction, in twenty-four hour format showing hours and minutes;
e) The date of the transaction, in any recognized format, indicating the day, month, and year; and
f) Unique validation number where, for wagering instruments that have yet to be redeemed, only the last four digits may be displayed by the Gaming Equipment.

**NOTE**: It is acceptable to have wagering instrument transactions recorded in separate logs or in a larger log which also contains records of other types of transactions (e.g., cashless transactions, bonusing transactions, promotional transactions, etc.).

## ~~4.7 Validation System Reports~~

### ~~4.7.1 General Statement~~

~~In addition to meeting the "General Reporting Requirements", the Validation System shall be capable of providing the necessary information to produce the reports listed in this section, unless properly communicated to another Gaming System, which will assume these responsibilities.~~

### ~~4.7.2 Meter Reconciliation Reports~~

~~The following information shall be provided to produce one or more reports for reconciling each Gaming Equipment's metered amounts against the Validation System's recorded amounts, as applicable:~~

~~a) Unique Gaming Equipment ID or equivalent;~~
~~b) Voucher In meter vs. system recorded voucher redemptions;~~
~~c) Voucher Out meter vs. vouchers system recorded voucher issuances;~~
~~d) Coupon Promotion In meter vs. system recorded coupon redemptions;~~
~~e) Coupon Promotion Out meter vs. system recorded coupon issuances; and~~
~~f) Any other information needed for reconciliation which is not covered by the above.~~

# *Appendix B: GLI Standards for Electronic Table Games*

## STANDARD SERIES

# GLI-24:

# Electronic Table Game Systems

**Version: 1.3**

**Release Date: September 6, 2011**

This Page Intentionally Left Blank

## ABOUT THIS STANDARD

This Standard has been produced by **Gaming Laboratories International, LLC** for the purpose of providing independent certifications to suppliers under this Standard and complies with the requirements set forth herein.

A supplier should submit equipment with a request that it be certified in accordance with this Standard. Upon certification, Gaming Laboratories International, LLC will provide a certificate of compliance evidencing the certification to this Standard.

# *Table of Contents*

# CHAPTER 1
## *1.0 STANDARD OVERVIEW*

### 1.1 Introduction

***1.1.1 General Statement***. **Gaming Laboratories International, LLC (GLI)** has been testing gaming equipment since 1989. Over the years, we have developed numerous standards for jurisdictions all over the world. In recent years, many jurisdictions have opted to ask for the development of industry standards without creating their own standards documents. In addition, with technology changing almost monthly, new technology is not being incorporated quickly enough into existing standards due to the long process of administrative rulemaking. This document, *GLI Standard 24*, will set forth the technical Standards for Electronic Table Game Systems (ETGS).

***1.1.2 Document History***. This document is an essay from many standards documents from around the world. Some GLI has written; some, such as the Australian and New Zealand National Standard, were written by Industry Regulators with input from test laboratories and electronic table game manufacturers. We have taken each of the standards' documents, merged each of the unique rules together, eliminating some rules and updating others, in order to reflect both the change in technology and the purpose of maintaining an objective, factual standard. We have listed below, and given credit to, agencies whose documents we reviewed prior to writing this Standard. It is the policy of **Gaming Laboratories International, LLC** to update this document as often as possible to reflect changes in technology, testing methods, or cheating methods. This document will be distributed without charge to all those who request it. It may be obtained by downloading it from our website at www.gaminglabs.com or by writing to us at:

**Gaming Laboratories International, LLC**
600 Airport Road
Lakewood, NJ 08701
(732) 942-3999 Tel
(732) 942-0043 Fax

## 1.2 Purpose of Technical Standards

***1.2.1*** ***General Statement***. The Purpose of this Technical Standard is as follows:

a) To eliminate subjective criteria in analyzing and certifying Electronic Table Game Systems operation.

b) To only test those criteria that impact the credibility and integrity of Electronic Table Game Systems from both the Revenue Collection and Player's perspective.

c) To create a standard that will ensure that the Electronic Table Game Systems are fair, secure, and able to be audited and operated correctly.

d) To distinguish between local public policy and laboratory criteria. At GLI, we believe that it is up to each local jurisdiction to set public policy with respect to gaming.

e) To recognize that non-gaming testing (such as Electrical Testing) should not be incorporated into this standard but left to appropriate test laboratories that specialize in that type of testing. Except where specifically identified in the standard, testing is not directed at health or safety matters. These matters are the responsibility of the manufacturer, purchaser, and operator of the equipment.

f) To construct a standard that can be easily changed or modified to allow for new technology.

g) To construct a standard that does not specify any particular method or algorithm. The intent is to allow a wide range of methods to be used to conform to the standards, while at the same time, to encourage new methods to be developed.

***1.2.2*** ***No Limitation of Technology***. One should be cautioned that this document should not be read in such a way that limits the use of future technology. The document should not be interpreted that if the technology is not mentioned, then it is not allowed. Quite to the contrary, as new technology is developed, we will review this standard, make changes and incorporate new minimum standards for the new technology.

## 1.3 Other Documents That May Apply

***1.3.1 General Statement***. The following other GLI standards may apply, depending on the features of the electronic table game system and references throughout this document. All GLI standards are available on our website at www.gaminglabs.com:.

a) GLI-11 Gaming Devices in Casinos;
b) GLI-12 Progressive Gaming Devices in Casinos;
c) GLI-13 On-Line Monitoring and Control Systems (MCS) and Validation Systems in Casinos;
d) GLI-16 Cashless Systems in Casinos;
e) GLI-17 Bonusing Systems in Casinos; and
f) GLI-18 Promotional Systems in Casinos.

*NOTE: This standard covers the Technical Specifications of the operation of Electronic Table Game Systems, as defined within section 1.4.1 below, where the table games are operated electronically without a live dealer. Please refer to GLI-25 for Electronic Table Game Systems that utilize a live dealer.*

## 1.4 Defining Electronic Table Game Systems

***1.4.1 General Statement***. An Electronic Table Game System (ETGS) is the combination of a Central Server, Player Interface and all Interface Elements that function collectively for the purpose of electronically simulating table game operations. **This standard is to be used when there is no live dealer and the game plays without significant human interaction** including the initiation of game play, responsible for all monetary transactions including credit acceptance, collecting wagers, distributing winnings, and ensuring all wagers are registered properly. **This standard will not make assumptions as to the classification of a device in a particular jurisdiction as being a table game or a gaming device, as defined within the GLI-11 Gaming Devices in Casinos standard. Nor does GLI offer an opinion as to how many 'devices' the equipment encompasses.**

*NOTE: For table game systems that utilize a live dealer please refer to the GLI Standard 25.*

## 1.5 Phases of Testing

***1.5.1*** ***General Statement***. Electronic Table Game submissions to the Test Laboratory will be performed in two phases:

a) Within the laboratory setting; and
b) On-site following the initial install of the system to ensure proper configuration of the security applications.

*NOTE: In addition to the on-site testing of the system, the Test Laboratory shall provide training on this new technology to the local regulators, recommended field auditing procedures, and assistance with the compilation of Internal Controls, if requested.*

# CHAPTER 2

## *2.0 ELECTRONIC TABLE GAME SYSTEM REQUIREMENTS*

### 2.1 Introduction

***2.1.1*** ***General Statement***. This chapter would apply to the overall system operations to ensure the security, accountability and integrity of the equipment.

### 2.2 Table Game System Requirements

***2.2.1*** ***System Clock***. The system must maintain an internal clock that reflects the current time (24hr format - which is understood by the local date/time format) and date that shall be used to provide for the following:

a) Time stamping of significant events;
b) Reference clock for reporting; and
c) Time stamping of configuration changes.

***2.2.2*** ***Synchronization Feature***. If multiple clocks are supported, the system shall have a facility whereby it is able to synchronize those clocks in each system component, whereby conflicting information could not occur.

## 2.3 System Security

***2.3.1*** ***General Statement***. All communications, including Remote Access, must pass through at least one approved application-level firewall and must not have a facility that allows for an alternate network path.

***2.3.2*** ***Firewall Audit Logs***. The firewall application must maintain an audit log of the following information and must disable all communications and generate an error event if the audit log becomes full:

a) All changes to configuration of the firewall;
b) All successful and unsuccessful connection attempts through the firewall; and
c) The source and destination IP Addresses, Port Numbers and MAC Addresses.

***2.3.3*** ***Surveillance/Security Functionality***. The system shall provide for interrogation that enables on-line comprehensive searching of the significant event log.

***2.3.4*** ***Access Control***. The system must support either a hierarchical role structure whereby user name and password define program access or individual menu item access or logon program /device security based strictly on user name and password or PIN. The system shall not permit the alteration of any significant log information without supervised access control. There shall be a provision for system administrator notification and user lockout or audit trail entry after a set number of unsuccessful login attempts. The system shall record: Date and Time of the Login attempt, username supplied, and success or failure. The use of generic user accounts on servers is not permitted.

***2.3.5*** ***Data Alteration***. The system shall not permit the alteration of any accounting or significant event log information without supervised access controls. In the event financial data is changed, an audit log must be capable of being produced to document:

a) Data element altered;
b) Data element value prior to alteration;
c) Data element value after alteration;
d) Time and Date of alteration; and
e) Personnel that performed alteration (user login).

## 2.4 Remote Access

***2.4.1*** ***Remote Access defined***. Remote Access defines any access made by a component outside the 'trusted' network.

***2.4.2*** ***General Statement***. Remote access where permitted, shall authenticate all computer systems based on the authorized settings of the electronic table game and firewall application that establishes a connection with the electronic table game as long as the following requirements are met:

a) Remote Access User Activity log is maintained by both the property and the manufacturer, depicting: authorized by, purpose, logon name, time/date, duration, and activity while logged in;
b) No unauthorized remote user administration functionality (adding users, changing permissions, etc.);
c) No unauthorized access to database;
d) No unauthorized access to operating system; and
e) If remote access is to be on a continuous basis then a network filter (firewall) must be installed to protect access (Dependent upon jurisdictional approval).

***2.4.3*** ***Self Monitoring***. The system must implement self monitoring of all critical Interface Elements (e.g. Central hosts, network devices, firewalls, links to third parties, etc.) and shall have the ability to effectively notify the system administrator of any error condition, provided the

condition is not catastrophic. The system shall be able to perform this operation with a frequency of at least once in every 24-hour period and during each power-up and power reset.

## 2.5 Backups and Recovery

***2.5.1 System Redundancy, Backup & Recovery***. The system shall have sufficient redundancy and modularity so that if any single component or part of a component fails, gaming can continue. There shall be redundant copies of each log file or system database or both on the system with open support for backups and restoration.

***2.5.2 Backup & Recovery***. In the event of a catastrophic failure when the system cannot be restarted in any other way, it shall be possible to reload the system from the last viable backup point and fully recover the contents of that backup, recommended to consist of at least the following information:

a) Significant events;
b) Accounting information;
c) Auditing information; and
d) Specific site information such as Device file, employee file, game profiles, etc

## 2.6 Communication Protocol

***2.6.1 General Statement***. Each component of an electronic table game system must function as indicated by the communication protocol implemented. All protocols must use communication techniques that have proper error detection and/or recovery mechanisms which are designed to prevent unauthorized access or tampering, employing Data Encryption Standards (DES) or equivalent encryption with secure seeds or algorithms. Any alternative measures will be reviewed on a case-by-case basis, with regulator approval.

## 2.7 System Integrity

***2.7.1 General Statement***. The Laboratory will perform certain tests to determine whether or not outside influences affect game fairness to the player or create cheating opportunities. This certification applies exclusively to tests conducted using current and retrospective methodology developed by Gaming Laboratories International, LLC (GLI). During the course of testing, GLI inspects for marks or symbols indicating that a device has undergone product safety compliance testing. Gaming Laboratories International, LLC also performs, where possible, a cursory review of submissions and information contained therein related to Electromagnetic Interference (EMI), Radio Frequency Interference (RFI), Magnetic Interference, Liquid Spills, Power Fluctuations and Environmental conditions. Electrostatic Discharge Testing is intended only to simulate techniques observed in the field being used to attempt to disrupt the integrity of electronic table game systems. Compliance to any such regulations related to the aforementioned testing is the sole responsibility of the device manufacturer. GLI claims no liability and makes no representations with respect to such non-gaming testing. An electronic table game system shall be able to withstand the following tests, resuming game play without operator intervention:

a) Random Number Generator If implemented, the random number generator and random selection process shall be impervious to influences from outside the device, including, but not limited to, electro-magnetic interference, electro-static interference, and radio frequency interference;

b) Electro-Static Interference. Protection against static discharges requires that the table game's conductive cabinets be earthed in such a way that static discharge energy shall not permanently damage or permanently inhibit the normal operation of the electronics or other components within the electronic table game. The electronic table game may exhibit temporary disruption when subjected to a significant electro-static discharge greater than human body discharge, but they shall exhibit a capacity to recover and complete any interrupted play without loss or corruption of any control or critical data information associated with the electronic table game. The tests will be conducted with a severity level of a maximum of 27KV air discharge;

***2.7.2 Physical Security***. The server or system component(s) must reside in a secure area where access is limited to authorized personnel. It is recommended that logical access to the game be logged on the system or on a computer or other logging device that resides outside the secure area and is not accessible to the individual(s) accessing the secure area. The logged data should include the time, date, and the identity of the individual accessing the secure area. The resulting logs should be kept for a minimum of 90 days.

## 2.8 Random Number Generator

***2.8.1 General Statement***. The Random Number Generator (RNG) is the selection of game symbols or production of game outcomes. The regulations within this section are only applicable to electronic table games that utilize an RNG, which shall:

a) Be statistically independent;
b) Conform to the desired random distribution;
c) Pass various recognized statistical tests; and
d) Be unpredictable.

***2.8.2 Game Selection Process***.

a) All Combinations and Outcomes Shall Be Available. Each possible permutation or combination of game elements that produces winning or losing game outcomes shall be available for random selection at the initiation of each play, unless otherwise denoted by the game.
b) No Near Miss. After selection of the game outcome, the electronic table game shall not make a variable secondary decision, which affects the result shown to the player. For instance, the random number generator chooses an outcome that the game will be a loser.
c) No Corruption from Associated Equipment. An electronic table game shall use appropriate protocols that effectively protect the random number generator and random

selection process from influence by associated equipment, which may be communicating with the electronic table game.

***2.8.3*** ***Applied Tests***. The test laboratory may employ the use of various recognized tests to determine whether or not the random values produced by the random number generator pass the desired confidence level of 99%. These tests may include, but are not limited to:

a) Chi-square test;
b) Equi-distribution (frequency) test;
c) Gap test;
d) Overlaps test;
e) Poker test;
f) Coupon collector's test;
g) Permutation test;
h) Kolmogorov-Smirnov test;
i) Adjacency criterion tests;
j) Order statistic test;
k) Runs tests (patterns of occurrences should not be recurrent);
l) Interplay correlation test;
m) Serial correlation test potency and degree of serial correlation (outcomes should be independent of the previous game);
n) Tests on subsequences; and
o) Poisson distribution.

***2.8.4*** ***Background RNG Activity***. The RNG shall be cycled continuously in the background between games and during game play at a speed that cannot be timed by the player. The test laboratory recognizes that some time during the game, the RNG may not be cycled when interrupts may be suspended. The test laboratory recognizes this but shall find that this exception shall be kept to a minimum.

***2.8.5 RNG Seeding***. The first seed shall be randomly determined by an uncontrolled event. After every game there shall be a random change in the RNG process (new seed, random timer, delay, etc.). This will verify the RNG doesn't start at the same value every time. It is permissible not to use a random seed; however, the manufacturer must ensure that games will not synchronize.

***2.8.6 Live Game Correlation***. Unless otherwise denoted on the pay glass/display, where the electronic table game plays a game that is recognizable such as Poker, Blackjack, Roulette, etc., the same probabilities associated with the live game shall be evident in the simulated game. For example, the odds of getting any particular number in Roulette where there is a single zero (0) and a double zero (00) on the wheel, shall be 1 in 38; the odds of drawing a specific card or cards in Poker shall be the same as in the live game.

***2.8.7 Card Games***. The requirements for games depicting cards being drawn from a deck are the following:

a) At the start of each game/hand, the cards shall be drawn fairly from a randomly-shuffled deck; the replacement cards shall not be drawn until needed, and in accordance with game rules, to allow for multi-deck and depleting decks;
b) Cards once removed from the deck shall not be returned to the deck except as provided by the rules of the game depicted;
c) As cards are removed from the deck they shall be immediately used as directed by the Rules of the Game (i.e., the cards are not to be discarded due to adaptive behavior by the electronic table game system)

*NOTE: It is acceptable to draw **random numbers** for replacement cards at the time of the first hand random number draw. Provided the replacement cards are sequentially used as needed.*

## 2.9 Maintenance of Critical Memory

***2.9.1 General Statement***. Critical memory storage may be maintained by the player terminal or the system, where applicable. Critical memory shall be maintained by a methodology that enables errors to be identified. This methodology may involve signatures, checksums, partial checksums, multiple copies, timestamps and/or effective use of validity codes.

*NOTE: The "Maintenance of Critical Memory" section is not intended to preclude the use of alternate storage media types, such as hard disk drives, for the retention of critical data. Such alternate storage media is still expected to maintain critical data integrity in a manner consistent with the requirements in this section, as applicable to the specific storage technology implemented.*

***2.9.2 Comprehensive Checks***. Comprehensive checks of critical memory shall be made following game initiation but prior to display of game outcome to the player. It is recommended that critical memory is continuously monitored for corruption. Test methodology shall detect failures with an extremely high level of accuracy.

***2.9.3 Unrecoverable Critical Memory***. An unrecoverable corruption of critical memory shall result in an error. The memory error shall not be cleared automatically and shall result in a tilt condition, which facilitates the identification of the error and causes the electronic table game to cease further function. *The critical memory error shall also cause any communication external to the electronic table game to immediately cease.* An unrecoverable critical memory error shall require a full non-volatile memory clear performed by an authorized person.

***2.9.4 Non-volatile Memory and Program Storage Device Space***. Non-volatile memory space that is not critical to the electronic table game operations are not required to be validated.

## 2.10 Program Storage Device Requirements

***2.10.1 General Statement***. The term *Program Storage Device* is defined to be the media or an electronic device that contains the critical control program components. Device types include but are not limited to EPROMs, compact flash cards, optical disks, hard drives, solid state drives, USB drives, etc. This partial list may change as storage technology evolves. All program storage devices shall:

a) Be housed within a fully enclosed and locked logic compartment;
b) Be clearly marked with sufficient information to identify the software and revision level of the information stored in the device. In the case of media types on which multiple programs may reside it is acceptable to display this information via the attendant menu.
c) Validate themselves during each processor reset; and
d) Validate themselves the first time they are used; and
e) CD-ROM, DVD, and other optical disk-based Program Storage shall:
    i. Not be a re-writeable disk; and
    ii. The "Session" shall be closed to prevent any further writing.

## 2.11 Control Program Requirements

***2.11.1 Control Program Verification***.

a) EPROM-based Program Storage:
    i. Electronic table games which have control programs residing in one or more EPROMs must employ a mechanism to verify control programs and data. The mechanism must use at a minimum a checksum; however, it is recommended that a Cyclic Redundancy Check (CRC) be used (at least 16-bit).
b) Non-EPROM Program Storage shall meet the following rules:
    i. The software shall provide a mechanism for the detection of unauthorized and corrupt software elements, upon any access, and subsequently prevent the

execution or usage of those elements by the electronic table game. The mechanism must employ a hashing algorithm which produces a message digest output of at least 128 bits.

ii. In the event of a failed authentication, after the game has been powered up, the electronic table game should immediately enter an error condition and display an appropriate error. This error shall require operator intervention to clear and shall not clear until; the data authenticates properly, following the operator intervention, or the media is replaced or corrected, and the electronic table game's memory is cleared.

*NOTE: Control Program Verification Mechanisms may be evaluated on a case-by-case basis and approved by the regulator and the independent testing laboratory based on industry standard security practices.*

c) Alterable Media shall meet the following rules in addition to the requirements outlined in 2.11.1(b):

i. Employ a mechanism which tests unused or unallocated areas of the alterable media for unintended programs or data and tests the structure of the media for integrity. The mechanism must prevent further play of the electronic table game if unexpected data or structural inconsistencies are found.

ii. Employ a mechanism for keeping a record anytime a control program component is added, removed, or altered on any alterable media. The record shall contain a minimum of the last ten (10) modifications to the media and each record must contain that date and time of the action., identification of the component affected, the reason for the modification and any pertinent validation information.

*NOTE: Alterable Program Storage does not include memory devices typically considered to be alterable which have been rendered "read-only" by either a hardware or software means.*

***2.11.2 Program Identification***. Program storage devices, which do not have the ability to be modified while installed in the electronic table game during normal operation, shall be clearly

marked with sufficient information to identify the software and revision level of the information stored in the devices.

***2.11.3 Independent Control Program Verification***. The system server(s) and each component of the electronic table game that would have an effect on the integrity of the electronic table game shall have the ability to allow for an independent integrity check of the device's software from an outside source and is required for all control programs that may affect the integrity of the game. This must be accomplished by being authenticated by a third-party device, which may be embedded within the game software (see NOTE below), by having an interface port for a third-party device to authenticate the media, or by allowing for removal of the media such that it can be verified externally. This integrity check will provide a means for field verification of the software to identify and validate the program. The test laboratory, prior to device approval, shall evaluate the integrity check method.

*NOTE: If the authentication program is contained within the game software, the manufacturer must receive written approval from the test laboratory prior to submission.*

## 2.12 Player Interface Terminal Requirements

***2.12.1 General Statement***. Player interface terminals may either be a display mechanism where the system performs all operations of the game (Thin Client), or contain its own logic function in conjunction with the electronic table game system (Thick Client). In either case, the player interface terminal(s) must meet the hardware and software requirements outlined within each jurisdiction's applicable requirements for gaming devices, to ensure security and player safety. In the absence of these jurisdictional specific requirements, the GLI-11 requirements should be used.

## 2.13 Rules of Play

### *2.13.1 Display.*

a) A placard or video display used to convey game play information shall be clearly identified and shall accurately state the house rules of the game, game profile and rake (collection) schedule, and the award that will be paid to the player when the player obtains a specific win.

b) The placard or video display shall clearly indicate whether awards are designated in denominational units, currency, or some other unit.

c) The table game shall reflect any change in award value, which may occur in the course of play. This may be accomplished with a digital display in a conspicuous location to the table game, and the table game must clearly indicate such.

d) All paytable information should be available to the player, prior to them committing to a bet. This includes unique game features, extended play, free spins, double-up, take-a-risk, auto play, countdown timers, symbol transformations, and community style bonus awards.

e) Placard or video displays shall not be certified if the information is inaccurate.

f) Any table game which utilizes multiple decks of cards should alert the player to the number of card decks in play.

### *2.13.2 Multi-Wager Games.*

a) Each individual wager to be played shall be clearly indicated on the player interface so that the player is in no doubt as to which wagers have been made; and

b) The winning outcome(s) shall be clearly discernable to the player. (e.g., on an Electronic terminal it may be accomplished by highlighting the symbol(s) or wagers and/or the flashing of winning symbol(s) or wagers. Where there are wins on multiple wagers, each winning wager may be indicated in turn.)

## 2.14 Software Requirements for Percentage Payout

***2.14.1 General Statement***. Each Electronic Table Game System shall theoretically payout a minimum of seventy-five percent (75%) during the expected lifetime of the game (i.e., progressives, bonus systems, merchandise, etc. shall not be included in the percentage payout if they are external to the game).

*NOTE: The laboratory will provide the minimum and maximum theoretical payout percentage for the game within the certification report, unless otherwise noted. Additional external awards added to a game will require a re-evaluation of the theoretical payout percentage, considering the value of the award and possibly other factors. The laboratory will re-evaluate a game's theoretical payout percentage when requested.*

a) Optimum Play Used for Skill Games. Electronic Table Game Systems that may be affected by player skill shall be calculated using a method of play that will provide the greatest return to the player over a period of continuous play.

b) Minimum Percentage Requirement Met at All Times. The minimum percentage requirement shall be met at all times. The minimum percentage requirement shall be met when playing at the lowest end of a non-linear paytable (i.e., if a game is continuously played at a minimum bet level for its total game cycle and the theoretical RTP is lower than the minimum percentage, then the game is unacceptable). This example also extends to games such as Keno, whereby the continuous playing of any spot combination results in a theoretical return to player lower than the minimum percentage.

c) Double-up or Gamble. The Double-up or Gamble options shall have a theoretical return to the player of one hundred percent (100%).

d) Additional or Optional Wagers. If these wagers can only be made by participating in the base game, the minimum and maximum payback percentage will be included with calculations of the base game.

***Please be advised, the above rules regarding payback percentage are not applicable for non-house banked Electronic Table Game Systems****

## 2.15 Player Interface Error Conditions

***2.15.1 General Statement***. The Player Interface, where applicable, shall be capable of detecting and displaying the following error conditions and illuminating a light system for each, or sound an audible alarm. Error conditions should cause the electronic table game to lock up and require attendant intervention except as noted within this section. Error conditions shall be cleared either by an attendant or upon initiation of a new play sequence after the error has cleared except for those denoted by an "*" which will require further evaluation since deemed as a critical error. Error conditions shall be communicated to an on-line monitoring and control system, where applicable:

***2.15.2 Door Open Error Conditions***.

a) All external doors on the electronic table game;
b) Drop box door;
c) Stacker door; and
d) Any other currency storage areas that have a door.

***2.15.3 Other Error Conditions***.

a) NV memory error (for any critical memory)*;
b) Low NV memory battery for batteries external to the NV memory itself or low power source;
c) Program error or authentication mismatch*;

***2.15.4 Error Codes***. For games that use error codes, a description of electronic table game error codes and their meanings shall be affixed inside the device. This does not apply to video-based games; however, video based games shall display meaningful text as to the error conditions.

## 2.16 Door Open/Close

***2.16.1 Required Door Metering***. The system or components of the system shall be able to detect and meter access to the following secure areas provided power is supplied to the device:

a) All external doors on the electronic table game;
b) Drop box door;
c) Stacker door; and
d) Any other currency storage areas that have a door.

## 2.17 Taxation Reporting Limits

***2.17.1 General Statement***. The game shall be capable of entering a lock up condition if any awards from a single game cycle are in excess of a limit that is required by a taxing jurisdiction. Notwithstanding the foregoing, it is permissible to provide a mechanism to accrue W2G eligible winnings to a separate meter. This meter must not provide for the ability to place wagers and when collected by the player must lockup as required by a taxing jurisdiction.

## 2.18 Play History

***2.18.1 Number Of Last Games Required***. For the purpose of settling disputes between players or players versus the house, the electronic table game system shall maintain the historical data for the play history. Information on at least the last ten (10) games/hands played is to be always retrievable on the operation of a suitable external key-switch, or another secure method that is not available to the player.

***2.18.2 Last Play Information Required***. Last play information shall provide all information required to fully reconstruct the last ten (10) games/hands played. All values shall be displayed, including the initial credits or ending credits, credits bet, credits won, and credits paid whether the outcome resulted in a win or loss. This information can be represented in graphical or text format. If a progressive was awarded, it is sufficient to indicate the progressive was awarded and not display the value. This information should include the final game outcome, including all player choices and bonus features. In addition, include the results of double-up or gamble (if applicable). For games that do not re-shuffle the cards at the beginning of each game, there must be secure procedures to permit a forced 're-shuffle' following access to the play history. These procedures are to be included in the system submission to the Test Laboratory.

*NOTE: For "Last Play Information" stated above, it is allowable to display values in currency in place of 'credits'.*

***2.18.3 Bonus Rounds***. The last play information shall reflect bonus rounds in their entirety. If a bonus round lasts 'x number of events,' each with separate outcomes, each of the 'x events' shall be displayed with its corresponding outcome, regardless if the result is a win or loss. Electronic table games offering games with a variable number of free games, per base game, may satisfy this requirement by providing the capability to display the last 50 free games in addition to each base game.

## 2.19 Significant Logs and Events

***2.19.1 General Statement***. Significant events are generated at the electronic table game and sent directly to the backend utilizing an approved Communication Protocol, as described in the earlier part of this document. All Significant Events that take place at each table will be monitored and recorded in an Event History. The Event History may be divided into sections (e.g. accounting, security, finance, errors, etc.); these events will be logged by date, time and event, and should be filterable. Each event must be stored in a database(s) which includes the following:

a) Date and time which the event occurred;
b) Identity of the electronic table game system component that generated the event;
c) A unique number/code that defines the event; or
d) A brief text that describes the event in the local language.

***2.19.2 Significant Events Defined***. The following events must be conveyed to the backend where a mechanism must exist for timely notification:

a) Power resets of any device;
b) Loss of communication with any device;
c) Error Conditions on any critical interface element;
d) Critical memory/control program corruption of any critical component.
e) Cashless account transactions,
f) Jackpots (W2G Reportable Events or Large Win Events)
g) Game start
h) Game stop
i) Software signature check and result (if supported)
j) Connection by authorized devices
k) Attempted connection by unauthorized devices

## 2.20 Accounting Information

***2.20.1 General Statement***. There shall be a method to accurately maintain the accounting information that is needed for proper revenue reporting and auditing. For electronic table game systems that do not maintain this information electronically, operational procedures are to be included with the system submission. Electronic table game systems that do maintain electronic accounting information shall effectively collect and store the information in a secure manner.

***2.20.2 Clearing Meters***. The clearing of stored Accounting Information may only be performed by authorized personnel via secure system controls or approved internal controls.

***2.20.3 Backup Requirements***. Data recorded by electronic meters shall be preserved after a power loss to an interface component and shall be maintained for a period of at least thirty (30) days.

## 2.21 Reports

***2.21.1 General Statement***. For electronic table game systems that maintain Significant Event and Accounting Information reports shall subsequently be available on demand. The reports must be generated accurately and provide effective information for the purpose of security and accounting auditing. For electronic table game systems that have the ability to communicate the Significant Event and Accounting Information to a separate Monitoring Control System it must be via a secure communication protocol.

***2.21.2 Cashless Transactions***. The following reports are required for electronic table game systems that provide for cashless transactions unless properly communicated to a separate Monitoring Control System

a) Patron Account Summary and Detail Reports. These reports shall include beginning and ending account balance, transaction information depicting machine number, amount, date/time and are to be immediately available to a patron upon request.
b) Liability Report. This report is to include previous day's starting value of outstanding Cashless Liability, aggregate Cashless-In and out totals (Including rake, jackpot and amount in play), and ending Cashless liability, if applicable.
c) Cashless Meter Reconciliation Summary and Detail Reports. These reports will reconcile each participating device's cashless Meter(s) against the Electronic Table Game System's cashless activity. (including Cashless in and Cashless out)

d) Cashier Summary and Detail Reports. To include patron account, Deposits and cash-out, amount of transaction, date and time of transaction, and cashier starting and ending balances, session start and end date/time (etc.) by cashier.

e) Device Transaction Summary and Detail Reports. Wagering, issuance, voids by device, date/time, account number, and transaction number.

f) Cashless Wagering System Activity Report. Deposits, transfers to and from electronic table game system, withdrawals, adjustments and balances, by wagering account.

g) Electronic Table Game System Performance Report. Hands per hour, total hands played, number of hours of operation, dollars played, dollars contributed and average number of players.

h) Cashless Wagering Account Adjustment Report. For each individual adjustment made to a cashless wagering account or a promotional account, a summary of the adjustment to include:

   i. Patron name and account number, or specific promotion, as applicable;
   ii. Amount of, and explanation for, the adjustment; and
   iii. Identification of the user completing and/or authorizing the adjustment.

## 2.22 Electronic Table Game Identification

***2.22.1 General Statement***. A electronic table game shall have an identification badge affixed to the exterior of the table by the manufacturer, that is not removable without leaving evidence of tampering and this badge shall include the following information:

a) The manufacturer;

b) A unique serial number;

c) The electronic table game model number; and

d) The date of manufacture.

## STANDARD SERIES

# GLI-25:

# Dealer Controlled Electronic Table Games

**Version: 1.2**

**Release Date: September 6, 2011**

This Page Intentionally Left Blank

## ABOUT THIS STANDARD

This Standard has been produced by **Gaming Laboratories International, LLC** for the purpose of providing independent certifications to suppliers under this Standard and complies with the requirements set forth herein.

A supplier should submit equipment with a request that it be certified in accordance with this Standard. Upon certification, Gaming Laboratories International, LLC will provide a certificate of compliance evidencing the certification to this Standard.

# *Table of Contents*

# CHAPTER 1
## *1.0 STANDARD OVERVIEW*

### 1.1 Introduction

***1.1.1 General Statement***. **Gaming Laboratories International, LLC (GLI)** has been testing gaming equipment since 1989. Over the years, we have developed numerous standards for jurisdictions all over the world. In recent years, many jurisdictions have opted to ask for the development of industry standards without creating their own standards documents. In addition, with technology changing almost monthly, new technology is not being incorporated quickly enough into existing standards due to the long process of administrative rulemaking. This document, *GLI Standard 25*, will set forth the technical Standards for Dealer Controlled Electronic Table Games (ETG).

***1.1.2 Document History***. This document is an essay from many standards documents from around the world. Some GLI has written; some, such as the Australian and New Zealand National Standard, were written by Industry Regulators with input from test laboratories and electronic table game manufacturers. We have taken each of the standards' documents, merged each of the unique rules together, eliminating some rules and updating others, in order to reflect both the change in technology and the purpose of maintaining an objective, factual standard. We have listed below, and given credit to, agencies whose documents we reviewed prior to writing this Standard. It is the policy of **Gaming Laboratories International, LLC** to update this document as often as possible to reflect changes in technology, testing methods, or cheating methods. This document will be distributed without charge to all those who request it. It may be obtained by downloading it from our website at www.gaminglabs.com or by writing to us at:

**Gaming Laboratories International, LLC**
600 Airport Road
Lakewood, NJ 08701
(732) 942-3999 Tel
(732) 942-0043 Fax

## 1.2 Purpose of Technical Standards

***1.2.1*** ***General Statement***. The Purpose of this Technical Standard is as follows:

a) To eliminate subjective criteria in analyzing and certifying Dealer Controlled Electronic Table Games.

b) To only test those criteria that impact the credibility and integrity of Dealer Controlled Electronic Table Games from both the Revenue Collection and Player's perspective.

c) To create a standard that will ensure that the Dealer Controlled Electronic Table Games are fair, secure, and able to be audited and operated correctly.

d) To distinguish between local public policy and laboratory criteria. At GLI, we believe that it is up to each local jurisdiction to set public policy with respect to gaming.

e) To recognize that non-gaming testing (such as Electrical Testing) should not be incorporated into this standard but left to appropriate test laboratories that specialize in that type of testing. Except where specifically identified in the standard, testing is not directed at health or safety matters. These matters are the responsibility of the manufacturer, purchaser, and operator of the equipment.

f) To construct a standard that can be easily changed or modified to allow for new technology.

g) To construct a standard that does not specify any particular method or algorithm. The intent is to allow a wide range of methods to be used to conform to the standards, while at the same time, to encourage new methods to be developed.

***1.2.2*** ***No Limitation of Technology***. One should be cautioned that this document should not be read in such a way that limits the use of future technology. The document should not be interpreted that if the technology is not mentioned, then it is not allowed. Quite to the contrary, as new technology is developed, we will review this standard, make changes and incorporate new minimum standards for the new technology.

## 1.3 Other Documents That May Apply

***1.3.1 General Statement***. The following other GLI standards may apply, depending on the features of the electronic table game and references throughout this document. All GLI standards are available on our website at www.gaminglabs.com:

a) GLI-11 Gaming Devices in Casinos;
b) GLI-12 Progressive Gaming Devices in Casinos;
c) GLI-13 On-Line Monitoring and Control Systems (MCS) and Validation Systems in Casinos;
d) GLI-16 Cashless Systems in Casinos;
e) GLI-17 Bonusing Systems in Casinos; and
f) GLI-18 Promotional Systems in Casinos.

*NOTE: This standard covers the Technical Specifications of the operation of Dealer Controlled Electronic Table Games, as defined within section 1.4.1 below, where the table games are operated electronically, that require interaction from a live dealer. Please refer to GLI-24 for Electronic Table Game Systems that do not utilize a live dealer.*

## 1.4 Defining Dealer Controlled Electronic Table Games

***1.4.1 General Statement***. Dealer Controlled Electronic Table Games (ETG) is the operation of a table game(s) that require a live dealer that utilizes electronics as part of the game's operation (i.e., game generation, electronically collecting, storing, communicating accounting and significant event data, etc.) **This standard is only to be used when the electronic table game requires a live dealer. This standard will not make assumptions as to the classification of a device in a particular jurisdiction as being a table game or a gaming device, as defined within the GLI-11 Gaming Devices in Casinos standard. Nor does GLI offer an opinion as to how many 'devices' the equipment encompasses.**

*NOTE: For table game systems that do not utilize a live dealer please refer to the GLI Standard 24.*

## 1.5 Phases of Testing

***1.5.1 General Statement***. Electronic table game submissions to the Test Laboratory may be performed in two phases:

a) Within the laboratory setting; and
b) On-site following the initial install of the system to ensure proper configuration of the security applications.

*NOTE: In addition to the on-site testing of the system, the Test Laboratory shall provide training on this new technology to the local regulators, recommended field auditing procedures, and assistance with the compilation of Internal Controls, if requested.*

# CHAPTER 2

## *2.0 ELECTRONIC TABLE GAME SYSTEM REQUIREMENTS*

### 2.1 Introduction

This chapter addresses electronic table game's that may or may not function as a component within a table game system. The regulations of each subchapter only apply when the electronic table game(s) operate as part of a 'table game system' that is independent of any external gaming system. Electronic table game's that operate in conjunction with external systems shall meet the game level and communication requirements established within the appropriate GLI Standard.

### 2.2 Table Game System Requirements

***2.2.1*** ***System Clock***. The system must maintain an internal clock that reflects the current time (24hr format - which is understood by the local date/time format) and date that shall be used to provide for the following:

a) Time stamping of significant events;
b) Reference clock for reporting; and
c) Time stamping of configuration changes.

***2.2.2*** ***Synchronization Feature***. If multiple clocks are supported the system shall have a facility whereby it is able to synchronize those clocks in each system component, whereby conflicting information could not occur.

## 2.3 System Security

***2.3.1*** ***General Statement***. All communications, including Remote Access, must pass through at least one approved application-level firewall and must not have a facility that allows for an alternate network path.

***2.3.2*** ***Firewall Audit Logs***. The firewall application must maintain an audit log of the following information and must disable all communications and generate an error event if the audit log becomes full:

a) All changes to configuration of the firewall;
b) All successful and unsuccessful connection attempts through the firewall; and
c) The source and destination IP Addresses, Port Numbers and MAC Addresses.

***2.3.3*** ***Surveillance/Security Functionality***. The system shall provide for interrogation that enables on-line comprehensive searching of the significant event log.

***2.3.4*** ***Access Control***. The system must support either a hierarchical role structure whereby user name and password define program access or individual menu item access or logon program /device security based strictly on user name and password or PIN. The system shall not permit the alteration of any significant log information without supervised access control. There shall be a provision for system administrator notification and user lockout or audit trail entry, after a set number of unsuccessful login attempts. The system shall record: Date and Time of the Login attempt, username supplied, and success or failure. The use of generic user accounts on servers is not permitted.

***2.3.5*** ***Data Alteration***. The system shall not permit the alteration of any accounting or significant event log information without supervised access controls. In the event financial data is changed, an audit log must be capable of being produced to document:

a) Data element altered;

b) Data element value prior to alteration;
c) Data element value after alteration;
d) Time and Date of alteration; and
e) Personnel that performed alteration (user login).

## 2.4 Remote Access

***2.4.1*** ***Remote Access defined***. Remote access defines any access made by a component outside the 'trusted' network.

***2.4.2*** ***General Statement***. Remote access where permitted, shall authenticate all computer systems based on the authorized settings of the electronic table game and firewall application that establishes a connection with the electronic table game as long as the following requirements are met:

a) Remote Access User Activity log is maintained by both the property and the manufacturer, depicting: authorized by, purpose, logon name, time/date, duration, and activity while logged in;
b) No unauthorized remote user administration functionality (adding users, changing permissions, etc.);
c) No unauthorized access to database;
d) No unauthorized access to operating system; and
e) If remote access is to be on a continuous basis then a network filter (firewall) must be installed to protect access (Dependent upon jurisdictional approval).

***2.4.3*** ***Self Monitoring***. The system must implement self monitoring of all critical Interface Elements (e.g. central hosts, network devices, firewalls, links to third parties, etc.) and shall have the ability to effectively notify the system administrator of any error condition, provided the condition is not catastrophic. The system shall be able to perform this operation with a frequency of at least once in every 24-hour period and during each power-up and power reset.

## 2.5 Backups and Recovery

***2.5.1*** ***System Redundancy, Backup & Recovery***. The system shall have sufficient redundancy and modularity so that if any single component or part of a component fails, gaming can continue. There shall be redundant copies of each log file or system database or both on the system with open support for backups and restoration.

***2.5.2*** ***Backup & Recovery***. In the event of a catastrophic failure when the system cannot be restarted in any other way, it shall be possible to reload the system from the last viable backup point and fully recover the contents of that backup, recommended to consist of at least the following information:

a) Significant events;
b) Accounting information;
c) Auditing information; and
d) Specific site information such as Device file, Employee file, game profiles, etc.

## 2.6 Communication Protocol

***2.6.1*** ***General Statement***. Each component of an electronic table game system must function as indicated by the communication protocol implemented. All protocols must use communication techniques that have proper error detection and/or recovery mechanisms which are designed to prevent unauthorized access or tampering, employing Data Encryption Standards (DES) or equivalent encryption with secure seeds or algorithms. Any alternative measures will be reviewed on a case-by-case basis, with regulator approval.

## 2.7 System Integrity

***2.7.1 General Statement***. The Laboratory will perform certain tests to determine whether or not outside influences affect game fairness to the player or create cheating opportunities. This certification applies exclusively to tests conducted using current and retrospective methodology developed by Gaming Laboratories International, LLC (GLI). During the course of testing, GLI inspects for marks or symbols indicating that a device has undergone product safety compliance testing. Gaming Laboratories International, LLC also performs, where possible, a cursory review of submissions and information contained therein related to Electromagnetic Interference (EMI), Radio Frequency Interference (RFI), Magnetic Interference, Liquid Spills, Power Fluctuations and Environmental conditions. Electrostatic Discharge Testing is intended only to simulate techniques observed in the field being used to attempt to disrupt the integrity of electronic table game systems. Compliance to any such regulations related to the aforementioned testing is the sole responsibility of the device manufacturer. GLI claims no liability and makes no representations with respect to such non-gaming testing. An electronic table game system shall be able to withstand the following tests, resuming game play without operator intervention:

a) Random Number Generator. If implemented, the random number generator and random selection process shall be impervious to influences from outside the device, including, but not limited to, electro-magnetic interference, electro-static interference, and radio frequency interference;

b) Electro-Static Interference. Protection against static discharges requires that the table game's conductive cabinets be earthed in such a way that static discharge energy shall not permanently damage, or permanently inhibit the normal operation of the electronics or other components within the electronic table game. The electronic table game may exhibit temporary disruption when subjected to a significant electro-static discharge greater than human body discharge, but they shall exhibit a capacity to recover and complete any interrupted play without loss or corruption of any control or critical data information associated with the electronic table game. The tests will be conducted with a severity level of a maximum of 27KV air discharge;

***2.7.2 Physical Security***. The server or system component(s) must reside in a secure area where access is limited to authorized personnel. It is recommended that logical access to the game be logged on the system or on a computer or other logging device that resides outside the secure area and is not accessible to the individual(s) accessing the secure area. The logged data should include the time, date, and the identity of the individual accessing the secure area. The resulting logs should be kept for a minimum of 90 days.

## 2.8 Random Number Generator

***2.8.1 General Statement***. The Random Number Generator (RNG) is the selection of game symbols or production of game outcomes. The regulations within this section are only applicable to electronic table games that utilize an RNG, which shall:

a) Be statistically independent;
b) Conform to the desired random distribution;
c) Pass various recognized statistical tests; and
d) Be unpredictable.

***2.8.2 Game Selection Process***.

a) All Combinations and Outcomes Shall Be Available. Each possible permutation or combination of game elements that produces winning or losing game outcomes shall be available for random selection at the initiation of each play, unless otherwise denoted by the game.
b) No Near Miss. After selection of the game outcome, the electronic table game shall not make a variable secondary decision, which affects the result shown to the player. For instance, the random number generator chooses an outcome that the game will be a loser.
c) No Corruption from Associated Equipment. An electronic table game shall use appropriate protocols that effectively protect the random number generator and random

selection process from influence by associated equipment, which may be communicating with the electronic table game.

***2.8.3 Applied Tests***. The test laboratory may employ the use of various recognized tests to determine whether or not the random values produced by the random number generator pass the desired confidence level of 99%. These tests may include, but are not limited to:

a) Chi-square test;
b) Equi-distribution (frequency) test;
c) Gap test;
d) Overlaps test;
e) Poker test;
f) Coupon collector's test;
g) Permutation test;
h) Kolmogorov-Smirnov test;
i) Adjacency criterion tests;
j) Order statistic test;
k) Runs tests (patterns of occurrences should not be recurrent);
l) Interplay correlation test;
m) Serial correlation test potency and degree of serial correlation (outcomes should be independent of the previous game);
n) Tests on subsequences; and
o) Poisson distribution.

***2.8.4 Background RNG Activity***. The RNG shall be cycled continuously in the background between games and during game play at a speed that cannot be timed by the player. The test laboratory recognizes that some time during the game, the RNG may not be cycled when interrupts may be suspended. The test laboratory recognizes this but shall find that this exception shall be kept to a minimum.

***2.8.5*** ***RNG Seeding***. The first seed shall be randomly determined by an uncontrolled event. After every game there shall be a random change in the RNG process (new seed, random timer, delay, etc.). This will verify the RNG doesn't start at the same value, every time. It is permissible not to use a random seed; however, the manufacturer must ensure that games will not synchronize.

***2.8.6*** ***Live Game Correlation***. Unless otherwise denoted on the pay glass/display, where the electronic table game plays a game that is recognizable such as Poker, Blackjack, Roulette, etc., the same probabilities associated with the live game shall be evident in the simulated game. For example, the odds of getting any particular number in Roulette where there is a single zero (0) and a double zero (00) on the wheel, shall be 1 in 38; the odds of drawing a specific card or cards in Poker shall be the same as in the live game.

***2.8.7*** ***Card Games***. The requirements for games depicting cards being drawn from a deck are the following:

a) At the start of each game/hand, the cards shall be drawn fairly from a randomly-shuffled deck; the replacement cards shall not be drawn until needed, and in accordance with game rules, to allow for multi-deck and depleting decks;
b) Cards once removed from the deck shall not be returned to the deck except as provided by the rules of the game depicted;
c) As cards are removed from the deck they shall be immediately used as directed by the rules of the game (i.e., the cards are not to be discarded due to adaptive behavior by the electronic table game system)

*NOTE: It is acceptable to draw* ***random numbers*** *for replacement cards at the time of the first hand random number draw. Provided the replacement cards are sequentially used as needed.*

## 2.9 Maintenance of Critical Memory

***2.9.1 General Statement***. Critical memory storage may be maintained by the player terminal or the system, where applicable. Critical memory shall be maintained by a methodology that enables errors to be identified. This methodology may involve signatures, checksums, partial checksums, multiple copies, timestamps and/or effective use of validity codes.

*Note: The "Maintenance of Critical Memory" section is not intended to preclude the use of alternate storage media types, such as hard disk drives, for the retention of critical data. Such alternate storage media is still expected to maintain critical data integrity in a manner consistent with the requirements in this section, as applicable to the specific storage technology implemented.*

***2.9.2 Comprehensive Checks***. Comprehensive checks of critical memory shall be made following game initiation but prior to display of game outcome to the player. It is recommended that critical memory is continuously monitored for corruption. Test methodology shall detect failures with an extremely high level of accuracy.

***2.9.3 Unrecoverable Critical Memory***. An unrecoverable corruption of critical memory shall result in an error. The memory error shall not be cleared automatically and shall result in a tilt condition, which facilitates the identification of the error and causes the electronic table game to cease further function. *The critical memory error shall also cause any communication external to the electronic table game to immediately cease.* An unrecoverable critical memory error shall require a full non-volatile memory clear performed by an authorized person.

***2.9.4 Non-volatile Memory and Program Storage Device Space***. Non-volatile memory space that is not critical to the electronic table game operations are not required to be validated.

## 2.10 Program Storage Device Requirements

***2.10.1 General Statement***. The term *Program Storage Device* is defined to be the media or an electronic device that contains the critical control program components. Device types include

but are not limited to EPROMs, compact flash cards, optical disks, hard drives, solid state drives, USB drives, etc. This partial list may change as storage technology evolves. All program storage devices shall:

a) Be housed within a fully enclosed and locked logic compartment;
b) Be clearly marked with sufficient information to identify the software and revision level of the information stored in the device. In the case of media types on which multiple programs may reside it is acceptable to display this information via the attendant menu.
c) Validate themselves during each processor reset;
d) Validate themselves the first time they are used; and
e) CD-ROM, DVD, and other optical disk-based Program Storage shall:
    i. Not be a re-writeable disk; and
    ii. The "Session" shall be closed to prevent any further writing.

## 2.11 Control Program Requirements

### *2.11.1 Control Program Verificatiom*.

a) EPROM-based Program Storage:
    i. Electronic table games which have control programs residing in one or more EPROMs must employ a mechanism to verify control programs and data. The mechanism must use at a minimum a checksum; however, it is recommended that a Cyclic Redundancy Check (CRC) be used (at least 16-bit).
b) Non-EPROM Program Storage shall meet the following rules:
    i. The software shall provide a mechanism for the detection of unauthorized and corrupt software elements, upon any access, and subsequently prevent the execution or usage of those elements by the electronic table game. The mechanism must employ a hashing algorithm which produces a message digest output of at least 128 bits.

ii. In the event of a failed authentication, after the game has been powered up, the electronic table game should immediately enter an error condition and display an appropriate error. This error shall require operator intervention to clear and shall not clear until; the data authenticates properly, following the operator intervention, or the media is replaced or corrected, and the electronic table game's memory is cleared.

*NOTE: Control Program Verification Mechanisms may be evaluated on a case-by-case basis and approved by the regulator and the independent testing laboratory based on industry standard security practices.*

c) Alterable Media shall meet the following rules in addition to the requirements outlined in 2.11.1(b):

i. Employ a mechanism which tests unused or unallocated areas of the alterable media for unintended programs or data and tests the structure of the media for integrity. The mechanism must prevent further play of the electronic table game if unexpected data or structural inconsistencies are found.

ii. Employ a mechanism for keeping a record anytime a control program component is added, removed, or altered on any alterable media. The record shall contain a minimum of the last ten (10) modifications to the media and each record must contain that date and time of the action., identification of the component affected, the reason for the modification and any pertinent validation information.

*NOTE: Alterable Program Storage does not include memory devices typically considered to be alterable which have been rendered "read-only" by either a hardware or software means.*

***2.11.2 Program Identification***. Program storage devices which do not have the ability to be modified while installed in the electronic table game during normal operation, shall be clearly marked with sufficient information to identify the software and revision level of the information stored in the devices.

***2.11.3 Independent Control Program Verification.*** The system server(s) and each component of the electronic table game that would have an effect on the integrity of the electronic table game shall have the ability to allow for an independent integrity check of the device's software from an outside source and is required for all control programs that may affect the integrity of the game. This must be accomplished by being authenticated by a third-party device, which may be embedded within the game software (see NOTE below), by having an interface port for a third-party device to authenticate the media, or by allowing for removal of the media such that it can be verified externally. This integrity check will provide a means for field verification of the software to identify and validate the program. The test laboratory, prior to device approval, shall evaluate the integrity check method.

*NOTE: If the authentication program is contained within the game software, the manufacturer must receive written approval from the test laboratory prior to submission.*

## 2.12 Player Interface Terminal Requirements

***2.12.1 General Statement***. Player interface terminals may either be a display mechanism where the system performs all operations of the game (Thin Client), or contain its own logic function in conjunction with the electronic table game system (Thick Client). In either case, the player interface terminal(s) must meet the hardware and software requirements outlined within each jurisdiction's applicable requirements for gaming devices, to ensure security and player safety. In the absence of these jurisdictional specific requirements, the GLI-11 requirements should be used.

*NOTE: Requirements that cannot be met as a result of manual intervention performed by the live dealer must be addressed in operational procedures and submitted to the Test Laboratory.*

# GLI STANDARD SERIES

# GLI-16:

## STANDARDS FOR CASHLESS SYSTEMS AND TECHNOLOGIES

**VERSION: 3.0**

**REVISION DATE: JULY 31, 2024**

# About This Standard

**Gaming Laboratories International, LLC (GLI)** has developed this technical standard for the purpose of providing independent technical analysis and/or certifications to gaming industry stakeholders indicating the state of compliance for gaming operations and systems with the requirements set forth herein.

Operators and suppliers are expected to provide documentation, credentials, and associated access to a production equivalent test environment with a request to the independent testing laboratory that it be evaluated in accordance with this technical standard. Upon the successful completion of testing, the independent testing laboratory will provide a certificate of compliance evidencing the certification to this standard.

GLI-16 should be viewed as a living document that will be tailored periodically to align with this developing industry over time as gaming implementations and operations evolve.

# Table of Contents

# Chapter 1: Introduction to Cashless Systems and Technologies

## 1.1 Introduction

### 1.1.1 General Statement

**Gaming Laboratories International, LLC (GLI)** has been testing gaming equipment since 1989. Over the years, GLI has developed numerous technical standards utilized by jurisdictions all over the world. This document, *GLI-16*, sets forth the technical standards for Cashless Systems and Technologies.

### 1.1.2 Document History

This document is a compilation based upon many standards documents from around the world. Some were written by GLI; others were written by industry regulators with input from independent test laboratories and gaming operators, developers, and suppliers. GLI has taken each of the standards documents and merged the unique rules, eliminated some rules and updated others, to reflect both the change in technology and the purpose of maintaining an objective standard that achieves common regulatory objectives without unnecessarily impeding technological innovation. It is the policy of GLI to update this document as often as warranted to reflect changes in technology and/or testing methods. This document will be distributed without charge and may be obtained by downloading it from the GLI website at www.gaminglabs.com or by contacting GLI at:

**Gaming Laboratories International, LLC.**
600 Airport Road
Lakewood, NJ 08701
Phone: (732) 942-3999
Fax: (732) 942-0043

### 1.1.3 Acknowledgment of Other Standards Reviewed

GLI acknowledges and thanks the regulatory bodies and other industry participants who have assembled rules, regulations, technical standards, and other documents which have been influential in the development of this document.

## 1.2 Purpose of Technical Standards

### 1.2.1 General Statement

The purpose of this technical standard is as follows:

a) To eliminate subjective criteria in the evaluation and certification of Cashless Systems and Technologies.
b) To assess the criteria that impacts the credibility and integrity of gaming from both revenue collection and player perspectives.
c) To establish a standard that will ensure gaming is fair, secure, auditable, and able to be operated correctly.

d) To distinguish between local public policies and Independent Test Laboratory criteria, acknowledging that it is the prerogative of each regulatory body to set its own public policies with respect to gaming.
e) To recognize that the evaluation of internal controls (such as anti-money laundering, financial, and business processes) employed by operators should not be incorporated into the laboratory testing of the standard. Instead, these should be addressed within operational audits performed for local jurisdictions.
f) To develop a standard that can be easily revised to allow for new technology.
g) To formulate a standard that does not specify any particular design, method, or algorithm, thereby allowing a wide range of methods to conform to the standards while simultaneously encouraging the development of new methods.

### 1.2.2 No Limitation of Technology

One should be cautioned that this document shall not be read in such a way that limits the use of future technology. This document should not be interpreted to mean that if the technology is not mentioned, then it is not allowed. On the contrary, GLI will periodically review this standard and update it to include minimum standards for any new and relevant technology.

### 1.2.3 Adoption and Observance

This technical standard can be adopted in whole or in part by any regulatory body that wishes to implement a comprehensive set of technical requirements for Cashless Systems and Technologies.

## 1.3 Other Documents That May Apply

### 1.3.1 Other GLI Standards

This technical standard covers the requirements for Cashless Systems and Technologies. Depending on the technology utilized by a system or technology, additional GLI technical standards may also apply.

**NOTE:** The entire family of GLI Standards is available free of charge at www.gaminglabs.com.

### 1.3.2 Minimum Internal Control Standards (MICS)

Implementing Cashless Systems and Technologies is a complex endeavor, necessitating the development of internal processes and procedures to ensure the cashless production environment is secure and controlled adequately. To that end, it is expected that a set of Minimum Internal Control Standards (MICS) will be established by the regulatory body to define the minimum required internal processes for the management and handling of cashless transactions as well as the requirements for internal control of any system or component software and hardware within the cashless production environment, and their associated accounts. The regulatory body's MICS may also include technical security controls and testing requirements for the cashless production environment.

### 1.3.3 Gaming Security Framework (GSF)

Adherence to the GLI Gaming Security Framework (GLI-GSF) is strongly recommended for Cashless Systems and Technologies. The GLI-GSF defines technical security controls and testing requirements, which will be assessed during evaluations of the cashless production environment. This includes, but is not limited to, operational process reviews critical to compliance, vulnerability and penetration testing of the external and internal infrastructure and applications handling sensitive information, and any other criteria set by the regulatory body.

**NOTE:** The GLI Gaming Security Framework is available free of charge at www.gaminglabs.com.

## 1.4 Interpretation of this Document

### 1.4.1 General Statement

This technical standard applies to Gaming Systems and technologies which allow players to participate in cashless gaming activities using an approved, securely protected authentication method, which accesses:

a) A player account at the Cashless System of the operator; or
b) A player's electronic payment account, provided that it allows for the identification of the account and the source of funds.

**NOTE:** The intent is to provide a framework to cover payment methods currently known and permitted by law.
**NOTE:** This technical standard does NOT apply to systems and technologies related to the issuance and redemption of wagering instruments (vouchers and/or coupons) or promotional accounts. For detailed standards applicable to these systems, please reference the *GLI-13 Standards for Monitoring and Control Systems and Validation Systems* and *GLI-18 Standards for Promotional Systems* as necessary.
**NOTE:** Cashless Systems which support promotional credits associated with player accounts shall meet the *GLI-18 Standards for Promotional Systems* in addition to this document.

### 1.4.2 Software Suppliers and Operators

The components of a cashless environment, although they may be constructed in a modular fashion, are intended to function cohesively.

a) Cashless Systems and Technologies may be developed to have configurable features; the final configuration of which depends on the options chosen by the operator. From a testing perspective, it might not be possible to test all of the configurable features of a cashless environment submitted by a software supplier in the absence of the final configuration chosen by the operator; however, the configuration that will be utilized in the cashless production environment shall be communicated to the independent test laboratory to facilitate creating a functionally equivalent test environment.
b) Because of the integrated nature of a cashless production environment, there are several requirements in this document which may apply to both operators and suppliers. In such cases, the collection of systems and technologies needed to meet these requirements will be considered to be the cashless environment and the individual entities providing them will need to meet such eligibility requirements as the regulatory bodies deem appropriate for performance of these requirements.

**NOTE:** This document is not intended to define which parties are responsible for meeting the requirements detailed herein. It is the responsibility of the stakeholders of each jurisdiction to determine how to best meet the requirements laid out in this document.

## 1.5 Testing and Auditing

### 1.5.1 Laboratory Testing

The independent test laboratory will test and certify the components of the Cashless Systems and Technologies in accordance with the chapters of this technical standard within a controlled test environment, where applicable. Unless otherwise directed by the regulatory body:

a) For unaltered commercial off-the-shelf (COTS) components, such as PCs or tablets, certification is not required; and
b) For modified off-the-shelf (MOTS) components, certification is required only to the modifications made to the components unless otherwise required by the regulatory body.

**NOTE**: Upon request, or as required by the regulatory body, the independent test laboratory will conduct on-site testing where the Cashless System, Cashless Devices, and communications are set-up prior to and/or during implementation.

### 1.5.2 Operational Audits and Assessments

The integrity and accuracy of the operation of Cashless Systems and Technologies is highly dependent upon operational procedures, configurations, and the cashless production environment's network infrastructure. In addition to the testing and certification of Cashless System and Technology components, a regulatory body may elect to require the following operational audits and assessments be conducted on a periodic basis:

a) An internal controls audit, against the applicable controls identified in the regulatory body's Minimum Internal Control Standards (MICS); and/or
b) A technical security assessment, against the applicable controls and tests identified in the GLI Gaming Security Framework (GLI-GSF), and/or any other controls and tests identified by the regulatory body.

# Chapter 2: Cashless System Requirements

## 2.1 Introduction

### 2.1.1 General Statement

A Cashless System may be entirely integrated into an existing Gaming System, such as a Monitoring and Control System, or exist as an entirely separate Gaming System. The requirements of this chapter apply to Cashless Systems in addition to the applicable "General Gaming System Requirements" within the *GLI-13 Standards for Monitoring and Control Systems and Validation Systems* and/or other applicable technical requirements observed by the regulatory body.

## 2.2 Cashless System Communications

### 2.2.1 Cashless Device Monitoring

The Cashless System shall be equipped to correctly read and store the applicable significant events and cashless transaction information, and specific cashless meter values from the Cashless Devices, according to the secure communication protocol implemented.

### 2.2.2 Interface Elements

Where Cashless Devices use Interface Elements to communicate with the Cashless System, the Interface Elements shall meet the applicable "Interface Element Requirements" within the *GLI-13 Standards for Monitoring and Control Systems and Validation Systems* and/or other applicable technical requirements observed by the regulatory body.

### 2.2.3 Cashless Transaction Communications

The Cashless System shall process cashless transactions correctly according to the secure communication protocol implemented.

## 2.3 Cashless Information to be Maintained

### 2.3.1 Information Retention

The Cashless System shall be capable of maintaining and backing up all applicable recorded information as discussed within this standard in addition to the "Information to be Maintained" within the *GLI-13 Standards for Monitoring and Control Systems and Validation Systems* and/or other applicable technical requirements observed by the regulatory body, unless properly communicated to another Gaming System, which will assume these responsibilities.

**NOTE**: Internal controls may be in place to ensure this information is recorded where it is not maintained directly by the system.

### 2.3.2 Cashless Significant Event Information

In addition to the "System Significant Event Information" within the *GLI-13 Standards for Monitoring and Control Systems and Validation Systems* and/or other applicable technical requirements observed by the regulatory body, cashless significant event information to be maintained and backed up shall include, as applicable:

a) Large cashless transactions (single and aggregate over defined time period) in excess of a value specified by the regulatory body, including transaction information;
b) For Cashless Systems which support player account management:
   i. Adjustments to a player account balance;
   ii. Changes made to sensitive information recorded in a player account;
   iii. Suspension or closure of a player account;
   iv. Large financial transactions (single and aggregate over defined time period) in excess of a value specified by the regulatory body, including transaction information; and
   v. Negative account balance (due to adjustments and/or chargebacks).

### 2.3.3 Cashless Transaction Information

The information to be maintained and backed up for each cashless transaction at a Cashless Device shall include, as applicable:

a) The type of transaction (e.g., transfer to/from Cashless Device, etc.);
b) The date and time of the transaction;
c) Unique transaction ID;
d) The transaction value;
e) Transaction status (pending, complete, etc.);
f) Unique Cashless Device ID or equivalent which handled the transaction; and
g) Unique player account ID, or for electronic payment accounts, an identifier which can be used to authenticate the type of account and the source of the funds (i.e., source of where funds came from/went to).

**NOTE:** This information may be useful to monitor Cashless Device activity, including but not limited to, identifying cashless transactions without associated game play.

### 2.3.4 Player Account Information

For Cashless Systems which support player account management, the information to be maintained and backed up for each player account shall include, as applicable:

a) Unique player account ID and username, if different;
b) The date and method from which the account was opened (e.g., remote vs. on-site), including relevant location information;
c) For verified player accounts:
   i. The personally identifiable information (PII) collected by the operator to register a player and create the account, including, their full legal name, date of birth, residential address, contact information, and any other information required by the operator or the regulatory body;

ii. The player's full or partial government identification number (social security number, taxpayer identification number, passport number, or equivalent), and their current and previous personal financial information (credit or debit instrument numbers, bank account numbers, etc.), which shall be encrypted or hashed to a cryptographic algorithm as allowed by the regulatory body;
iii. The date and method of identity verification, including, where applicable, a description of the identification credential provided by a player to confirm their identity and its date of expiration;
iv. The date of player agreement to the operator's terms and conditions and privacy policies, including the versions agreed upon;
v. Previous accounts, if any, and reason for closure;

d) The account's current and previous authentication credentials, which shall be encrypted or hashed to a cryptographic algorithm as allowed by the regulatory body:
e) Account details and current balance. All discretionary account funds shall be maintained separately;
f) The date and time of account is accessed by any person (player or operator), including relevant location information;
g) Where supported, limitation/time-out/suspension information as required by the regulatory body:
   i. The date and time of the request;
   ii. Description and reason of limitation/time-out/suspension;
   iii. The type of limitation/time-out/suspension (e.g., system-imposed weekly deposit limitation, twenty-four-hour time-out, self-imposed monthly deposit limitation, self-imposed temporary suspension);
   iv. The date and time limitation/time-out/suspension commenced;
   v. The date and time limitation/time-out/suspension ended;
h) Financial transaction information:
   i. The type of transaction (e.g., deposit, withdrawal, adjustment, etc.);
   ii. The date and time of the transaction;
   iii. Unique transaction ID;
   iv. Amount of transaction;
   v. Total account balance before/after transaction;
   vi. Total amount of fees paid for transaction, if any;
   vii. Unique Cashless Device ID or equivalent which handled the transaction;
   viii. Transaction status (pending, complete, etc.);
   ix. Method of deposit/withdrawal (e.g., cash, personal check, cashier's check, wire transfer, money order, credit or debit instrument, electronic payment account, etc.);
   x. Deposit authorization number;
   xi. Relevant location information.
i) The date and method from which the account was closed (e.g., remote vs. on-site), including relevant location information and reason for closure;
j) The current status of the player account (e.g., active, inactive, closed, suspended, etc.).

**NOTE:** This information may be useful to monitor player account activity, including but not limited to, identifying account openings and closings in short time frames and deposits and withdrawals without associated game play.

## 2.4 Cashless System Reports

### 2.4.1 General Statement

In addition to meeting the "General Reporting Requirements" within the *GLI-13 Standards for Monitoring and Control Systems and Validation Systems*, the Cashless System shall be capable of providing the necessary information to produce the reports listed in this section, unless properly communicated to another Gaming System, which will assume these responsibilities.

### 2.4.2 Meter Reconciliation Reports

The following information shall be provided to produce one or more reports for reconciling each Cashless Device's metered amounts against the Cashless System's recorded amounts, as applicable:

a) Unique Cashless Device ID or equivalent;
b) Electronic Funds Transfer In (EFT In) meter vs. system recorded EFT In transactions;
c) Player Account Transfer In (WAT In) meter vs. system recorded WAT In transactions;
d) Player Account Transfer Out (WAT Out) meter vs. system recorded WAT Out In transactions; and
e) Any other information needed for reconciliation which is not covered by the above.

### 2.4.3 Player Account Reports

For Cashless Systems which support player account management, the following reports shall be able to be produced for player accounts, as applicable:

a) Player Account Activity Reports. These reports are to include, for each player account, balance, deposit and withdrawal amounts, transfers to and from Cashless Devices, and adjustments (single transaction amounts and aggregate amounts); and
b) Player Account Liability Reports. These reports are to include, for each gaming day, the starting liability amount (total amount held by the operator for player accounts), total additions and subtractions to account balances, and the ending liability.

### 2.4.4 Cashier Summary and Detail Reports

The following information shall be provided to produce one or more reports for each cashier session at a Cashier Station which performs financial transactions for player accounts:

a) Unique Cashier Station ID or equivalent;
b) User account ID or name of cashier;
c) The date and time the cashier session began and ended;
d) The cashier balances at the start and end of the cashier session;
e) For each financial transaction:
    i. Unique transaction ID;
    ii. Unique player account ID;
    iii. The type of transaction (e.g., deposit, withdrawal, adjustment, etc.);
    iv. The transaction value;
    v. The date and time of the transaction; and
f) The cashier balance at the end of the cashier session (blank until known).

# Chapter 3: Cashless Device Requirements

## 3.1 Introduction

### 3.1.1 General Statement

The requirements throughout this chapter apply to kiosks, gaming devices, electronic table games, electronic wager stations, live game management components, and any other critical gaming equipment maintained by the operator and used in the cashless environment, also known as Cashless Devices. Any additional device or software which is used to meet a regulatory requirement may also be subject to these requirements based on functionality.

## 3.2 Device Requirements

### 3.2.1 Identifying a Cashless Device

A player should be able to identify each Cashless Device by a means left to the discretion of the regulatory body (e.g., remove display menu items that pertain to cashless functionality for gaming equipment not participating; provide a host message indicating cashless capability; or a specific sticker on the gaming equipment to indicate participation or non-participation).

### 3.2.2 Configuring Cashless Transactions

Since cashless functionality would impact the electronic accounting meters, it shall not be possible to change a configuration setting that causes any obstruction or alteration to these meters without performing an NV memory clear.

### 3.2.3 Diagnostic Tests on a Cashless Device

Controls shall be in place for any diagnostic functionality available at the Cashless Device such that all activity shall be reported to the Cashless System that would reflect the specific account(s) and the individual(s) tasked to perform these diagnostics. This would allow all cashless diagnostic activity that affects the Cashless Device's associated electronic accounting meters to be audited.

## 3.3 Player Identification Components

### 3.3.1 General Statement

A player identification component is software and/or hardware used with a Cashless Device which supports a means for players to provide identification information and/or the source of funds. This includes components which are controlled by a Cashless Device's critical control program and Interface Element-based or non-integrated form of these components that operate outside the control of the Cashless Device. Examples of these components include card readers, barcode readers, and biometric scanners.

### 3.3.2 General Component Requirements

Player identification components shall be electronically-based and be constructed in a manner that ensures proper handling of inputs and that protects against vandalism, abuse, or fraudulent activity. In addition, player identification components shall meet the following rules:

a) The player identification component shall be designed to prevent manipulation that may impact integrity and shall provide a method to enable the software to interpret and act appropriately upon a valid or invalid input;
b) Acceptance of any identification information shall only be possible when the Cashless Device is enabled for use. Other states, such as error conditions including door opens, shall cause the disabling of the player identification component; and
c) Any player identification component which locally stores information relating to cashless transactions shall not have means to compromise such information and shall not allow the removal of its information until that information has been successfully transferred and acknowledged by the Cashless System.

### 3.3.3 Card Reader

Card reader software shall be able to detect the use of a valid card, as applicable. The card reader shall be electronically based and be configured to ensure that it only reads valid cards.

### 3.3.4 Barcode Reader

Barcode reader software shall be able to associate the barcode visible on a card or an allowed software application on a player's mobile device (such as a smartphone or tablet), as applicable, with data stored in an external database as a means to identify and validate an account association, or for the purpose of redemption.

### 3.3.5 Biometric Scanner

Biometric scanner software shall be able to associate a person's physical characteristics with those recorded within an external database as means to authenticate the identity of a player and for the purpose of account association.

### 3.3.6 Wireless Device

Software which controls communication between a Cashless Device and any wireless devices that are conducted using contactless transmission technologies such as Near Field Communications (NFC), Bluetooth (BT), Wi-Fi, optical, etc., shall:

a) Utilize secure communication methods to prevent unauthorized access to sensitive information by unintended recipients;
b) Employ a method to detect data corruption; upon detection of corruption, either correct the error, or terminate the communication while providing a suitable error message;
c) Employ a method to prevent unauthorized modification of sensitive information that impacts device integrity or that represents secure player data; and
d) Only be possible with authorized player identification components.

**NOTE**: The independent test laboratory will make every attempt to ensure secure communications are employed and document attempts to intervene on communications.

### 3.3.7 Smart Card/Device Technology

If allowed by the regulatory body, players may access their accounts using smart card/device technology, including smartphone and tablet technology where the account information, including the current account balance, is maintained in the Cashless System's database. Smart cards/devices which have the ability to maintain a player account balance are only permissible when the Cashless System validates that the amount on the card/device agrees with the amount stored within the system's database (i.e., smart cards/devices cannot maintain the only source of account data).

**NOTE**: Smart card/device technology implementation will be evaluated on a case-by-case basis.

### 3.3.8 Hardware Location

The player identification component hardware shall be secured in a locked enclosure or sealed casing or located within a locked area of the Cashless Device (i.e., an area that requires opening of the main door for access). Only the areas of the component that require physical interaction shall be accessible to the player.

### 3.3.9 Error Conditions

The Cashless Device shall have mechanisms to interpret and act upon an error condition related to a malfunction of any player identification component, including communication failures. If a player identification component error condition is identified, the Cashless Device shall display an appropriate error message and disable the player identification component. This error condition shall be communicated to the connected system when such a compatible system and protocol is supported.

## 3.4 Cashless Transactions

### 3.4.1 Cashless Transaction Authentication

All cashless transactions between a supporting Cashless Device and the Cashless System shall be secured using a method of authentication, such as credit or debit instrument, card insertion or "tap" (contactless) capacity on the player identification component, a similar approved process that allows for the authentication of the account and the source of funds if a software application on a player's mobile device is used, or a secure alternative means (e.g., finger-print recognition). Authentication methods are subject to the discretion of the regulatory body as necessary. The requirement does not prohibit the option for more than one method of authentication being available for a player to access their account. Cashless transactions are entirely electronic.

a) An explanatory message shall be displayed to the player if there is an authentication failure (e.g., account is not recognized, invalid PIN, etc.).
b) Current account balance information shall be available to the player once authenticated. All discretionary account funds shall be indicated separately.

### 3.4.2 Transaction Messages

A confirmation/denial message shall be displayed to the player whenever any cashless transaction is being processed, including:

a) The type of transaction (e.g., transfer to/from Cashless Device, etc.);
b) The transaction value; and
c) For denied transactions, a descriptive message as to why the transaction did not complete as initiated.

### 3.4.3 Player Account Transfers

If the Cashless Device and the Cashless System support the ability to transfer funds between the player account and the Cashless Device for game play, the following shall apply:

a) After the player's identity is confirmed, funds may be transferred from their account balance to the Cashless Device's credit meter for game play. This may be automatic where the account balance is automatically transferred to the Cashless Device's credit meter or the player is presented transfer options, which require selection before occurring. Such options would include how much the player wishes to transfer to the Cashless Device's credit meter;
b) A transfer shall not be accepted that could cause the player to have a negative account balance. Where the account balance is less than the amount requested by the player, a transfer of the available funds may be processed provided that the player is clearly notified that they have transferred less than requested;
c) The account balance is to be debited when the transfer is accepted by the Cashless System and funds are added to the Cashless Device's credit meter;
d) Once game play is completed, the player shall have the option to transfer some or all of their funds on the Cashless Device's credit meter back to their account balance or cash-out their funds via voucher issuance or another method. Funds may not be transferred from the Cashless Device to a different player account; and
e) Any funds on the Cashless Device that are attempted to be transferred to a player account on the Cashless System that result in a communication failure for which this is the only available payout medium (the player cannot cash-out via voucher issuance or another method), shall result in a handpay lockup or tilt on the Cashless Device.

### 3.4.4 Direct Account Wagering

If the Cashless Device and the Cashless System support the ability to directly wager from the player account balance (i.e., funds are not transferred between the player account and the Cashless Device), the following shall apply:

a) A wager shall not be accepted that could cause the player to have a negative account balance;
b) The account balance is to be debited when the wager is accepted by the Cashless System; and
c) The amounts won from game play shall automatically update the account balance or be available for further wagering or cash-out via voucher issuance or another method.

### 3.4.5 Electronic Funds Transfers

Where allowed by the regulatory body, cashless transactions may be performed using an electronic payment account. In the event of an electronic funds transfer to the Cashless Device, the Cashless System shall:

a) Execute the transfer in accordance with all applicable jurisdictional electronic funds transfer requirements or other cashless transaction requirements including receipting and fee disclosure requirements; and
b) Not execute the transfer upon notification from the player's financial institution or third-party financial services provider that the available funds associated with the player's electronic payment account are less than the amount requested by the player. Alternatively, a transfer of the available funds may be processed provided that the player is clearly notified that they have transferred less than requested.

**NOTE**: The regulatory body may require electronic funds transfers to the Cashless Device to be performed in conjunction with a verified player account.

### 3.4.6 Transaction Limits

If a player initiates a cashless transaction and that transaction would exceed Cashless Device or System configured limits (i.e., the credit limit, transaction limit, etc.) or any limit that has been established for purposes of responsible gaming then this transaction may only be processed provided that the player is clearly notified that they have transacted less than requested to avoid player disputes.

### 3.4.7 Loss of Communication

If communication with the Cashless System is lost, the Cashless Device shall cease operations related to that communication, and a message shall be displayed to the player that cashless transactions cannot currently be processed. It is permissible for the Cashless Device to detect this error when the device tries to communicate with the system.

## 3.5 Cashless Meters and Logs

### 3.5.1 Information Access

The cashless meters and transaction logs required by this section shall have the ability to be displayed on demand using an authorized access method to ensure that only authorized personnel are allowed access. The meters and logs may be maintained locally by the Cashless Device and/or by an external critical component which records these meters and logs.

### 3.5.2 Cashless Meters

Electronic accounting meters shall be at least ten digits in length. Eight digits shall be used for the integer currency (e.g., dollar) amount and two digits used for the sub-currency (e.g., cents) amount. The meters shall automatically roll over to zero once its maximum logical value has been reached. Meters shall be labeled so they can be clearly understood in accordance with their function.

a) The required electronic accounting meters for each Cashless Device are as follows:
   i. Electronic Funds Transfer In (EFT In). There shall be a meter that accumulates the total value of cashable player funds electronically transferred to the Cashless Device from a financial institution or third-party financial services provider through a Cashless System or through the secure interface that uses a defined protocol;
   ii. Player Account Transfer In (WAT In). There shall be a meter that accumulates the total value of cashable player funds electronically transferred to the Cashless Device from a player account through a Cashless System or through the secure interface that uses a defined protocol. This meter does not include transfers of promotional credits;
   iii. Player Account Transfer Out (WAT Out). There shall be a meter that accumulates the total value of cashable player funds electronically transferred from the Cashless Device to a player account through a Cashless System or through the secure interface that uses a defined protocol. This meter does not include transfers of promotional credits;
   iv. Other Meters. Cashless transactions that would not otherwise be metered under any of the above meters, shall be recorded on sufficient meters to properly reconcile all such transactions.
b) The operation of other mandatory meters for Cashless Devices shall not be impacted directly by cashless transactions.

**NOTE:** Any accounting meter that is not supported by the functionality of the Cashless Device is not required to be implemented by the supplier.

### 3.5.3 Cashless Transaction Log

There shall be the capacity to display a complete transaction log for the previous thirty-five transactions that incremented any of the "Cashless Meters". The following information shall be displayed:

a) The type of transaction (e.g., transfer to/from Cashless Device, etc.);
b) The transaction value in local monetary units in numerical form;
c) The time of day of the transaction, in twenty-four hour format showing hours and minutes;
d) The date of the transaction, in any recognized format, indicating the day, month, and year; and
e) Unique player account ID, or for electronic payment accounts, an identifier which can be used to authenticate the type of account and the source of the funds (i.e., source of where funds came from/went to) where only the last four digits may be displayed by the Cashless Device.

**NOTE**: It is acceptable to have cashless transactions recorded in separate logs or in a larger log which also contains records of other types of transactions (e.g., bonusing transactions, promotional transactions, wagering instrument transactions, etc.).

# Chapter 4: Player Account Requirements

## 4.1 Introduction

### 4.1.1 General Statement

The requirements of this chapter apply to player accounts supported by the Cashless System and maintained by the operator. This chapter does not apply to electronic payment accounts.

## 4.2 Verified Player Accounts

### 4.2.1 General Statement

The requirements of this section apply to registration, activation, and updates to verified player accounts where such functionality is supported directly by the Cashless System.

### 4.2.2 Player Account Registration

Prior to the establishment of a verified player account, there shall be a method to collect player's personally identifiable information (PII) for the registration process. During the registration process, the player shall:

a) Be denied the ability to register for a player account if they submit a birth date which indicates that they are underage;
b) If not all fields are required, be informed on the registration form which information fields are "required", which are not, and what will be the consequences of not filling in the required fields;
c) Agree to the terms and conditions for accessing and using the player account and the privacy policies for PII protection;
d) Acknowledge that they are prohibited from allowing any unauthorized person to access or use their player account;
e) Consent to the monitoring and recording of the use of their player account by the operator and the regulatory body; and
f) Affirm that the PII the player is providing to open the player account is accurate.

**NOTE**: A player may hold only one active player account at a time unless specifically authorized by the regulatory body.

### 4.2.3 Identity Verification

Identity verification shall be undertaken before a verified player account is established. Third-party identity verification service providers may be used for identity verification.

a) Identity verification shall authenticate the player's full legal name, date of birth, and full or partial government identification number (driver's license number, social security number, taxpayer identification number, passport number, or equivalent) as required by the regulatory body.
b) Identity verification shall also confirm that the player is not on any exclusion lists held by the operator or the regulatory body or prohibited from establishing or maintaining an account for any other reason.

c) Details of identity verification shall be kept in a secure manner.

**NOTE**: Additional identity verification checks may be conducted throughout the lifetime of the verified player account if the operator has reasonable suspicion that the player's identification has been compromised.

### 4.2.4 Account Activation

The verified player account can only be established once age and identity verification are successfully completed, the player is determined to not be on any exclusion lists or prohibited from establishing or maintaining an account for any other reason, the player has acknowledged the necessary terms and conditions and privacy policies, and the player account registration is complete.

**NOTE**: When the terms and conditions and/or privacy policies are materially updated (i.e., beyond any grammatical or other minor changes), the player shall agree to their updates.

### 4.2.5 Account Updates

The player shall have the ability to access and update player account authentication credentials, registration information and the accounts used for financial transactions as supported by the system. Where supported, a multi-factor authentication process may be employed for account updates without gaming attendant involvement.

## 4.3 Unverified Player Accounts

### 4.3.1 General Statement

If supported by the Cashless System, unverified player accounts may be used where allowed by the regulatory body.

### 4.3.2 Account Balance Limits

If required by the regulatory body, the Cashless System shall enforce a maximum balance limit on the unverified player account.

a) Deposits may not occur which cause the player account balance to exceed this limit; and
b) If the player account's balance exceeds this limit due to game play, adjustments, or any other additions to the balance, the system shall then suspend the account from play until the balance is reduced to a value equal to or less than the maximum balance limit at a Kiosk or Cashier Station.

## 4.4 Player Account Management

### 4.4.1 Player Account Access at the System

In addition to the authentication methods mentioned for "Cashless Transaction Authentication", a player account may be accessed at the Cashless System using authentication credentials, such as a username (or similar) and a password or a secure alternative means to perform authentication to log in.

a) If the system does not recognize the authentication credentials provided, an explanatory message shall be displayed. The error message shall be the same regardless of which authentication credential is incorrect.
b) The player account shall be automatically locked-out after three successive failed active access attempts in a thirty-minute period, or a period to be determined by the regulatory body. Where supported, a multi-factor authentication process may be employed for a verified player account to be unlocked without attendant involvement. Alternatively, the system may, as supported, automatically release a locked-out account after thirty minutes, or a period to be determined by the regulatory body, has elapsed.
c) The system shall support a mechanism that allows for a player account to be locked-out or suspended in the event that other suspicious activity is detected. Where supported, a multi-factor authentication process may be employed for a verified player account to be unlocked without attendant involvement.
d) Where supported, a multi-factor authentication process may be employed for a player to retrieve or reset of their forgotten authentication credentials without gaming attendant involvement.

### 4.4.2 Financial Transactions

As supported, funds may be deposited to or withdrawn from the player account via a Cashier Station or any supporting Cashless Device (through coins/tokens, bills, wagering instruments, credit or debit instruments, etc.) or from an approved secure interface that uses a defined protocol or similar software application on a player's mobile device (such as a smartphone or tablet) that complies with the requirements with respect to player identification and source of funds. Where financial transactions can be performed automatically by the Cashless System the following requirements shall be met:

a) The system shall provide confirmation/denial of every financial transaction initiated, including
   i. The type of transaction (deposit/withdrawal);
   ii. The transaction value; and
   iii. For denied transactions, a descriptive message as to why the transaction did not complete as initiated.
b) Funds deposited into a player account shall not be available for wagering until they are received from the issuer or the issuer provides an authorization number indicating that the funds are authorized. The authorization number is to be maintained in an audit log.
c) Where financial transactions are allowed through Electronic Funds Transfers (EFT), there shall be security measures and controls in place to prevent EFT fraud. A failed EFT attempt may not be considered fraudulent if the player has successfully performed an EFT on a previous occasion with no outstanding chargebacks. Otherwise, the player account shall:
   i. Be temporarily locked-out for investigation of fraud after five consecutive failed EFT attempts within a ten-minute time period or a period to be determined by the regulatory body. If there is no evidence of fraud, the account may be unlocked; and
   ii. Have its access suspended after five additional consecutive failed EFT attempts within a ten-minute period or a period to be determined by the regulatory body.
d) Positive player identification or authentication shall be completed before the withdrawal of any funds can be made by the player. Where supported, a multi-factor authentication process may be employed for a player to withdraw funds without gaming attendant involvement.

e) The system shall employ a mechanism that can detect and prevent any withdrawal activity initiated by a player that would result in a negative account balance. Where payment processing issues outside the control of the system cause an account to be overdrawn, the player account shall be suspended until the negative account balance is settled.
f) Payments from an account are to be paid (including funds transfer) directly to an account with a financial institution or third-party financial services provider in the name of the player or made payable to the player and forwarded to the player's residential address using a secure delivery service or through another method that is not prohibited by the regulatory body. For verified player accounts, the name and residential address are to be the same as held in player registration details.
g) If a player initiates a financial transaction and that transaction would exceed limits put in place by the operator and/or regulatory body, this transaction may only be processed provided that the player is clearly notified that they have withdrawn or deposited less than requested.
h) It shall not be possible to transfer funds between two player accounts.
i) Security or authorization procedures shall be in place to ensure that only authorized adjustments can be made to player account balances, and these changes are auditable.

### 4.4.3 Transaction Log or Account Statement

The Cashless System shall be able to provide a transaction log or account statement history to a player upon request. The information provided shall include sufficient information to allow the player to reconcile the statement or log against their own financial records. Information to be provided shall include at a minimum, details on the following types of financial and cashless transactions (time stamped with a unique transaction ID) within the past year or other time period as requested by the player or as required by the regulatory body:

a) Deposits to the player account;
b) Withdrawals from the player account;
c) Funds added to/removed from the account balance from game play;
d) Manual adjustments or modifications to the account balance (e.g., due to refunds); and
e) Any other additions to, or deductions from, the account balance that would not otherwise be metered under any of the above-listed items.

**NOTE:** Where supported by the system, the player's self-imposed limitation, time-out, and suspension history may also be included.

### 4.4.4 Account Closure

Players shall be provided with a method to close their player account at any time unless the operator has suspended the player account. Any cashable player funds remaining in a player account shall be refunded to the player, provided that the operator acknowledges that the funds have cleared.

## 4.5 Limitations, Time-Outs, and Suspensions

### 4.5.1 General Statement

The requirements in this section apply where the Cashless System supports the ability to directly manage and implement limitations, time-outs, and/or suspensions.

### 4.5.2 Limitations

Players shall be provided with a method to impose limitations for account activity including, but not limited to deposits and cashless transactions over a defined time period (e.g., day, week, month) as required by the regulatory body. In addition, there shall be a method for the system to impose any limitations for account activity as required by the regulatory body.

a) Once established by a player and implemented by the system, it shall only be possible to reduce the severity of self-imposed limitations after the time period of the previous limit has expired, or as required by the regulatory body.
b) Players shall be notified in advance of any system-imposed limits and their effective dates. Once updated, system-imposed limits shall be consistent with what is disclosed to the player.
c) Upon receiving any self-imposed or system-imposed limitation order, the system shall ensure that all specified limits are implemented immediately or at the point in time (e.g., next login, next day) clearly indicated to the player.
d) The self-imposed limitations set by a player shall not override more restrictive system-imposed limitations. The more restrictive limitations shall take priority.
e) Limitations shall not be compromised by internal status events, such as time-outs or self-imposed suspension orders and revocations.

### 4.5.3 Time-Outs

Players shall be provided with a method to establish a time-out period up to seventy-two hours. In addition, there shall be a method for the operator to impose a time-out period on a player. During a timeout period, players may not conduct deposits and cashless transactions other than transferring funds from the Cashless Device back to their player account.

### 4.5.4 Suspensions

Players shall be provided with a method to suspend their player account for a specified period, which shall not be less than seventy-two hours, or indefinitely, as required by the regulatory body. In addition, there shall be a method for the operator to suspend a player account as required by the regulatory body. While a player account is suspended:

a) The player shall be given a notification that the account is suspended, the restrictions placed on the account, and general instructions for resolution where possible.
b) The player shall be prevented from:
    i. Performing cashless transactions other than transferring funds from the Cashless Device back to their player account;
    ii. Depositing funds with the exception of settling a negative account balance; and
    iii. Making changes to or closing their player account, unless authorized by the operator.
c) The player shall not be prevented from withdrawing any or all of their cashable player funds, provided that the operator acknowledges that the funds have cleared, and that the reasons for suspension would not prohibit a withdrawal.

# Glossary of Key Terms

**Algorithm** – A finite set of unambiguous instructions performed in a prescribed sequence to achieve a goal, especially a mathematical rule or procedure used to compute a desired result. Algorithms are the basis for most computer programming.

**Authentication** – Verifying the identity of a user, process, software package, or device, often as a prerequisite to allowing access to resources in a system.

**Barcode** – An optical machine-readable representation of data, including interleaved 2 of 5 barcodes, quick response (QR) codes, or any other machine-readable codes found on wagering instruments and cards.

**Barcode Reader** – A device that is capable of reading or interpreting a barcode. This may extend to some smartphones or other electronic devices that can execute an application to read a barcode.

**Biometric** – A biological identification input, such as fingerprints or retina patterns.

**BT, *Bluetooth*** – A low power, short-range wireless communications protocol utilized for the interconnection of cellular phones, computers, and other electronic devices, including Cashless Devices. Bluetooth connections typically operate over distances of ten meters or less and rely upon short-wavelength radio waves to transmit data over the air.

**Card Reader** – A device that reads data embedded on a magnetic strip, or stored in an integrated circuit chip, for player identification.

**Cashable Player Funds –** Player funds that are redeemable for cash, including cashable promotional credits.

**Cashable Promotional Credits** (aka "Unrestricted Promotional Credits") – Promotional credits that are redeemable for cash.

**Cashless Device** – An electronic device which facilitates financial transactions with a player account and/or cashless transactions between a player account or electronic payment account and Gaming Equipment maintained by the operator and used in the cashless environment. Any additional device or software which is used to meet a regulatory requirement may also be subject to control based on functionality.

**Cashless System** – The hardware, software, firmware, communications technology, other equipment, as well as operator procedures implemented in order to allow players to participate in wagering activities using an approved authentication method, which accesses a player account at the Cashless System of the operator or an electronic payment account of the player provided that it allows for the identification of the account and the source of funds. The system provides the operator with the means to review player accounts, generate various cashless/financial transaction and account reports, and set any configurable parameters.

**Cashless Transactions** – The electronic transfer to/from a Cashless Device of a player account's funds using a Cashless System. The term also includes direct account wagering and electronic funds transferred from an electronic payment account to a Cashless Device.

**Communications Technology** – Any method used, and the components employed, to facilitate the transmission and receipt of information, including transmission and reception by systems using wire, wireless, cable, radio, microwave, light, fiber optics, satellite, or computer data networks, including the Internet and intranets.

**Critical Component** – Any sub-system for which failure or compromise can lead to loss of player entitlements, government revenue or unauthorized access to data used for generating reports for the regulatory body.

**Critical Control Program** – A software program that controls behaviors relative to any applicable technical standard and/or regulatory requirement.

**Debit Instrument** – A card, code, or other device with which a person may initiate an electronic funds transfer from their electronic payment account or a player account transfer. The term includes, without limitation, a prepaid access instrument.

**Direct Account Wagering** – Cashless transactions involving wagers placed directly from the player account balance, and amounts won from game play added directly to the player account balance, as supported.

**Discretionary Account Funds** – Non-cashable promotional credits and promotional credits that have a possible expiration.

**EFT, *Electronic Funds Transfer*** (aka "ECT", "Electronic Credits Transfer") – A financial transaction or cashless transaction involving an electronic transfer of funds between an electronic payment account and a player account or from an electronic payment account to a Cashless Device through a Cashless System. This includes Automated Clearing House (ACH) transfers.

**Electronic Accounting Meter** (aka "Software Meter" / "Soft Meter") – An accounting meter that is implemented in Cashless Device software.

**Electronic Payment Account** – An account maintained with a financial institution or third-party financial services provider, such as PayPal, Google Pay, or Apple Pay, for the purposes of making electronic funds transfers. The term does not include a player account, or any other account held by an operator and used for gaming purposes.

**Electronic Table Game** – The combination of hardware and software components that function collectively to electronically simulate a live table game or a live card game. An electronic table game may be fully-automated or dealer-controlled (semi-automated).

**Electronic Wager Station –** A player interface unit that permits player transactions and/or wagering to be conducted at a live game.

**Gaming Device** – An electronic or electro-mechanical device that at a minimum will utilize an element of chance, skill, or strategy, or some combination of these elements in the determination of prizes, contain some form of activation to initiate the selection process, and makes use of a suitable methodology for delivery of the determined outcome.

**Gaming Equipment** – A gaming device, electronic table game, electronic wager station, live game management component, kiosk, or any other critical electronic gaming component and its Interface Element intended for use with a Gaming System.

**Gaming Venue** – A physical location or site where gaming activities take place, such as casinos, racetracks, card rooms, bingo halls, gaming halls, or other similar facilities where Gaming Equipment is installed, such as public establishments used for video lottery and other forms of distributed gaming.

**Interface Element** (aka "SMIB, *Slot Machine Interface Board")* – A circuit board that interfaces the Cashless Device with the Cashless System, supporting protocol conversion between the device and the system.

**Internet** – An interconnected system of networks that connects computers around the world via TCP/IP.

**Key** – A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification.

**Kiosk** – A player interface unit that may be used to perform regulated operations when interfaced with a compatible host Gaming System.

**Live Game** – A game conducted by a gaming attendant (e.g., dealer, croupier, etc.). Live games include, but are not limited to, live drawings, live card games, live table games, live keno games, live bingo games, and live play of other games as allowed by the regulatory body.

**Live Game Management Component** – A workstation for gaming attendants (e.g., dealer, croupier, etc.) to manage live game activity, such as a live table game or a live card game.

**Multi-Factor Authentication** – A type of authentication which uses two or more of the following to verify a user's identity: Information known only to the user (e.g., a password, pattern, or answers to challenge questions); An item possessed by a user (e.g., an electronic token, physical token, or an identification card); A user's biometric data (e.g., fingerprints, facial or voice recognition).

**NFC, *Near Field Communication*** – A short-range wireless connectivity standard that uses magnetic field induction to enable communication between devices when they are touched together or brought within a few centimeters of each other.

**Non-Cashable Promotional Credits** (aka "Restricted Promotional Credits") – Promotional credits that are not redeemable for cash.

**Operator** – A person or entity that oversees a cashless environment and/or maintains player accounts using both the technological capabilities of the Cashless System as well as their own internal control procedures.

**Password** – An authentication credential, using a string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

**PII, *Personally identifiable information*** – Sensitive information that could potentially be used to identify a particular player. Examples include a full legal name, date of birth, place of birth, government identification number (driver's license number, social security number, taxpayer identification number, passport number, or equivalent), residential address, phone number, email address, personal financial information (credit or debit instrument numbers, bank account numbers, etc.), or other personal information if defined by the regulatory body.

**PIN, *Personal Identification Number*** – An authentication credential, using a numerical code associated with an individual and which allows secure access to a domain, account, network, system, etc.

**Player Account** (aka "Wagering Account" / "Cashless Account") – An account maintained by an operator for a player where information relative to financial and cashless transactions are recorded on behalf of the player including, but not limited to, deposits, withdrawals, wagers, winnings, and balance adjustments. The term does not include an electronic payment account, or an account used solely by an operator to track promotional points or credits, or similar benefits issued by an operator to a player which may be redeemed for merchandise and/or services.

**Player Account Transfer** (aka "Wagering Account Transfer" / "Cashless Account Transfer") –A cashless transaction where cashable player funds are electronically transferred between the Cashless Device and a player account.

**Player Identification Component** – Software and/or hardware used with a Cashless Device which supports a means for players to provide identification information and/or the source of funds. Examples include a card reader, a barcode reader, or a biometric scanner.

**Prepaid Access Instrument** – A card, code, electronic serial number, mobile identification number, personal identification number or similar device used in conjunction with a Cashless System that allows player access to funds that have been paid in advance and can be retrieved or transferred at some point in the future through such a device.

**Promotional Award –** An award that is redeemable for cash or promotional credits based on predefined player activity criteria that is based on predefined player activity that are tied to a specific promotional account or other predefined criteria that do not require player or gaming activity prior to redemption and are generally single instance use.

**Promotional Credits** – Cashable promotional credits and non-cashable promotional credits.

**Protocol** – A set of rules and conventions that specifies information exchange between devices, through a network or other media.

**Risk** – The likelihood of a threat being successful in its attack against a network or system.

**Secure Communication** – Communication that provides the appropriate confidentiality, authentication, and content integrity protection.

**Sensitive Information** – Information that shall be handled in a secure manner, such as PII, gaming data, validation numbers, authentication credentials, PINs, passwords, secure seeds and keys, and other data which is of a sensitive nature.

**Smart Card/Device** – A card with embedded integrated circuits, or other technology, that possesses the means to electronically store or retrieve account data.

**Tilt** – An error in Cashless Device operation that halts or suspends operations and/or that generates some intelligent fault message.

**Time Stamp** – A record of the current value of the Cashless System date and time which is added to a message at the time the message is created.

**Unauthorized Access** – A person gains logical or physical access without permission to a network, system, application, data, or other resource.

**Unverified Player Account** – A player account which has not gone through the age and identity verification process.

**Verified Player Account** – A player account which is registered to a player and has gone through the age and identity verification process.

**Wi-Fi** – The standard wireless local area network (WLAN) technology for connecting computers and electronic devices to each other and/or to the internet.

**Workstation –** An interface for gaming attendants and other authorized personnel to access the regulated functions of the Cashless System. Examples of workstations include, but are not limited to, Cashier Stations and Live Game Management Components.