GLI STANDARD SERIES

GLI-33:

STANDARDS FOR EVENT WAGERING SYSTEMS

VERSION: 1.1 PUBLIC COMMENT DRAFT

REVISION DATE: APRIL 3, 2019

About This Standard

This technical standard has been produced by **Gaming Laboratories International, LLC (GLI)** for the purpose of providing independent technical analysis and/or certifications to wagering industry stakeholders indicating the state of compliance for wagering operations and systems with the requirements set forth herein.

This document is intended to be used by regulatory bodies, operators, and industry suppliers as a compliance guideline for technologies pertaining to Event Wagering Systems. This standard is not intended to represent a set of prescriptive requirements that every Event Wagering System must comply with; however, it does establish a technical standard regarding the technologies used to facilitate these operations. It should be stressed that some of the technical standards addressed within this document may be satisfied through manual operational controls as approved by each regulatory body.

An operator is expected to provide internal control documentation, credentials and associated access to a production equivalent test environment with a request that it be evaluated in accordance with this technical standard. Upon completion of testing, GLI will provide a certificate of compliance evidencing the certification to this Standard.

GLI-33 should be viewed as a living document that provides a level of guidance that will be tailored periodically to align with this developing industry over time as wagering 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 must 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 Specifications (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 must 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 must 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, must be performed at a frequency specified by the regulatory body:

a) Appendix A: Operational Audit of Event Wagering Procedures. 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, 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: Event Wagering Requirements

2.1 Introduction to Event Wagering Requirements

2.1.1 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.

2.2 Wagering Displays and Information

2.2.1 Posting of Wagering Rules

Comprehensive wagering rules must 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" section of this document.

2.2.2 Dynamic Information on Wagering Displays

The following information must 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 must be displayed as accurately as possible within the constraints of communication delays and latencies.

2.3 Wager Placement

2.3.1 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 must only be placed in conjunction with a player account.

2.3.2 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 must be straightforward, with all selections (including their order, if relevant) identified. When the wager involves multiple events (e.g., parlays), such groupings must be identified.
b) Players must have the ability to select the market they want to place a wager on.
c) Wagers must not be automatically placed on behalf of the player without the player's consent/authorization.
d) Players must 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 must 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 must be provided that a wager has been accepted or rejected (in full or in part). Each wager must 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 must be readily accessible.
    ii. A wager may 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.

2.3.3 Wager Record

Upon completion of a wagering transaction, the player must 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.

2.3.4 Wagering Period Close

It must not be possible to place wagers once the wagering period has closed.

2.3.5 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 must not mislead the player about the odds/payouts available in the paid version.

2.4 Results and Payment

2.4.1 Results Display

Results entry must include the entry of all information which may affect the outcome of all types of wagers offered for that event.

a) It must 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) must be made available.

2.4.2 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.

2.4.3 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 must 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 must 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 must 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 must update the database.

2.5 Virtual Event Wagering

2.5.1 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 applicable *GLI-11 Standards for Gaming Devices* as or jurisdictional requirements observed by the regulatory body.

2.5.2 Randomization and Virtual Events

A cryptographic RNG must be utilized to determine virtual event outcomes and must 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 *GLI-11 Standards for Gaming Devices* must be used as applicable. Additionally, the evaluation of virtual event outcomes using an RNG must comply with the following rules:

a) Where more than one RNG is used to determine different virtual event outcomes, each RNG must be separately evaluated; and
b) Where each instance of an RNG is identical, but involves a different implementation within the virtual event, each implementation must be separately evaluated.

2.5.3 Virtual Event Selection Process

Determination of events of chance that result in a monetary award may 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 must 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 may not limit the outcomes available for selection, except as provided for by design;
c) The virtual event may not modify or discard outcomes selected by the RNG due to adaptive behavior. Additionally, outcomes must 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 must 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 may 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 may 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 may not contain any logic utilized to generate the result of any virtual event. All critical functions including the generation of any virtual event must be generated by the Event Wagering System and be independent of the Wagering Device.

2.5.4 Virtual Event Display

Displays for a virtual event must 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 must be displayed to the player. It must 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 must 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 must be visually distinct from each other.
d) The result of a virtual event must 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.

2.5.5 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 must 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 must apply to the simulation:

a) The probability of any event occurring in the simulation that affects the outcome of the virtual event must 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 must 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 must be independent of their previous behavior, so as to be non-adaptive and non-predictable, unless otherwise disclosed to the player.

2.5.6 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 must 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.

2.6 External Wagering Systems

2.6.1 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.

2.6.2 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 must 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 must 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 must 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.

2.6.3 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 must 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 must 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 must 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 must be debited an amount equaling the offer and cost to the host wagering system. The funds must 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 must be made to the "pending" account and the account balance.
e) Cancellation requests from the guest wagering system must 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 cancelled wager.

2.6.4 Results

When results are entered and confirmed on the host wagering system, each winning wager must be transferred to the guest wagering system with the amount of the win. Confirmation of receipt of the winning wagers must be acknowledged by the guest wagering system.

Chapter 3: Wagering Device Requirements

3.1 Introduction to Wagering Device Requirements

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 must 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 must 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 must 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 must meet the following requirements:

a) The functions of all buttons, touch or click points must be clearly indicated within the area of the button, or touch/click point or within the help menu. There must 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 must 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, must be clearly communicated to the user and must not be misleading or inaccurate.
d) The display of the instructions and information must 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 must 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 must 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 must 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 must 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 requirements established within the *GLI-20 Standards for Kiosks* or other applicable jurisdictional requirements observed by the regulatory body must 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 must be met for POS Wagering Devices.

3.4.2 Touch Screen Displays

Touch screen displays, if in use by the Wagering Software, must be accurate, and if required by their design, must support a calibration method to maintain that accuracy; alternatively, the display hardware may support automatic self-calibration.

3.4.3 Wagering Instruments

POS Wagering Devices which support the issuance and/or redemption of wagering instruments (vouchers and coupons) must meet the applicable jurisdictional requirements for these items. In the absence of specific jurisdictional standards, the requirements established within the "Machine Vouchers" section of *GLI-11 Standards for Gaming Devices* and the "Voucher Validation System Requirements" of *GLI-13 Standards for On-Line Monitoring and Control Systems (MCS) and Validation Systems* must be used as applicable.

3.4.4 Printing Wager Records

If the POS Wagering Device connects to a printer to produce printed wager records and/or wagering instruments, the printer and/or Wagering Software must 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.

3.4.5 Wireless POS Wagering Devices

For portable POS Wagering Devices, the applicable requirements for "Client-Server Interactions" of the next section must also be met. Additionally, communication must only occur between the

portable 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 must 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 must not automatically alter any device-specified firewall rules to open ports that are blocked by either a hardware or software firewall;
c) The software must 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 must not alter the software's integrity in any way;
e) The software must not possess the ability to override the volume settings of the Remote Wagering Device; and
f) The software must 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 must 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 must prevent wagering operations and display an appropriate error message.

3.5.4 Content

Wagering Software must 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 Mandatory Player Account Use

Player account registration and verification are required by the Event Wagering System for a player to participate in remote wagering. The Event Wagering System must meet the "Player Account Management" requirements and "Player Account Controls" specified within this document.

3.5.6 Cookies

Where cookies are used, players must 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 must contain no malicious code.

3.5.7 Information Access

The Wagering Software must 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";
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: System Server Requirements

4.1 Introduction to System Server Requirements

4.1.1 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 must conform to the applicable technical requirements within this document.

4.2 System Clock Requirements

4.2.1 System Clock

The Event Wagering System must maintain an internal clock that reflects the current date and time that must 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.

4.2.2 Time Synchronization

The Event Wagering System must be equipped with a mechanism to ensure the time and dates between all components that comprise the system are synchronized.

4.3 Control Program Requirements

4.3.1 General Statement

In addition to the requirements contained within this section, the auditing procedures indicated in the "Verification Procedures" section of this document must also be met.

4.3.2 Control Program Self-Verification

The Event Wagering System must 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 must:

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.

4.3.3 Control Program Independent Verification

Each critical control program component of the Event Wagering System must have a method to be verified via an independent third-party verification procedure. The third-party verification process must operate independently of any process or security software within the system. The independent test laboratory, prior to system approval, must approve the integrity check method.

4.3.4 Shutdown and Recovery

The Event Wagering System must 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.

4.4 Event Wagering Management

4.4.1 Event Wagering Management

The Event Wagering System must 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).

4.5 Player Account Management

4.5.1 General Statement

The requirements of this section apply to player account management where supported by the Event Wagering System.

4.5.2 Registration and Verification

There must 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 must 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 must 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 must authenticate the legal name, physical address and age of the individual at a minimum as required by the regulatory body.
    ii. Identity verification must 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 must 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 must allow the ability to update passwords, registration information and the account used for financial transactions for each player. A multi-factor authentication process must be employed for these purposes.

4.5.3 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 must 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 must be employed for the retrieval of the username/resetting of the password.
c) Current account balance information and transaction options must be available to the player once authenticated.
d) After 30 minutes of inactivity on a specific Wagering Device, or a period determined by the regulatory body, the system must require a player to re-authenticate in order to access their account. No further wagering or financial transactions are permitted until the player has been re-authenticated.
e) The system may allow a simpler means for a player to re-authenticate, 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.

f) The system must 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 must be employed for the account to be unlocked.

4.5.4 Limitations and Exclusions

The Event Wagering System must 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 must be evaluated;
b) The self-imposed limitations set by a player must not override more restrictive operator-imposed limitations. The more restrictive limitations must take priority; and
c) Limitations must not be compromised by internal status events, such as self-imposed exclusion orders and revocations.

4.5.5 Player Funds Maintenance

Where financial transactions can be performed automatically by the Event Wagering System the following requirements must be met:

a) The system must 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 must 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 must not be possible to transfer funds between two player accounts.

4.5.6 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.) must be explained to the player;
b) The player must manually opt in to use this functionality (i.e., it must not be set by default); and
c) The player shall be able to opt out at any time.

4.5.7 Transaction Log or Account Statement

The Event Wagering System must be able to provide a transaction log or account statement history to a player upon request. The information provided must include sufficient information to allow the player to reconcile the statement or log against their own financial records. Information to be provided must 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.

4.5.8 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 must apply:

a) All awards must be equally available to all players who achieve the defined level of qualification for player loyalty points;
b) Redemption of player loyalty points earned must be a secure transaction that automatically debits the points balance for the value of the prize redeemed; and
c) All player loyalty points transactions must be recorded by the system.

4.6 Location Requirements for Remote Wagering

4.6.1 General Statement

Where required by the regulatory body, the requirements within this section must apply when the Event Wagering System supports remote wagering.

NOTE: The operator or third-party service provider maintaining these components, services and/or applications must meet the auditing procedures indicated in the "Location Service Provider" section of this document.

4.6.2 Location Fraud Prevention

The Event Wagering System must 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 must 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).

4.6.3 Location Detection for Remote Wagering on a WLAN

Where remote wagering occurs over a Wireless Local Area Network (WLAN), the Event Wagering System must 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 must 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.

4.6.4 Location Detection for Remote Wagering Over the Internet

Where remote wagering occurs over the internet, the Event Wagering System must 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 must 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 must be rejected, and the player shall be notified of this.
   ii. An entry must 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 must be used to provide a player's physical location and an associated confidence radius. The confidence radius must be entirely located within the permitted boundary.
c) Accurate location data sources (Wi-Fi, GSM, GPS, etc.) must 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 must 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 must 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 must be utilized.

4.7 Information to be Maintained

4.7.1 Data Retention and Time Stamping

The Event Wagering System must be capable of maintaining and backing up all recorded data as discussed within this section:

a) The system clock must be used for all time stamping.
b) The system must provide a mechanism to export the data for the purposes of data analysis and auditing/verification (e.g., CSV, XLS).

4.7.2 Wager Record Information

For each individual wager placed by the player, the information to be maintained and backed up by the Event Wagering System must 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);

4.7.3 Market Information

For each individual market available for wagering, the information to be maintained and backed up by the Event Wagering System must 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 for cancelled wagers, 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.

4.7.4 Contest/Tournament Information

For Event Wagering Systems which support contests/tournaments, the information to be maintained and backed up by the Event Wagering System must 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.).

4.7.5 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 must 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;

4.7.6 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 must include for each player account:

a) Unique player ID and player name;
b) Player data (including verification method);
c) 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) 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. Date exclusion/limitation commenced;
    v. 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.

4.7.7 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 must 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.

4.7.8 Significant Event Information

Significant event information to be maintained and backed up by the Event Wagering System must 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) 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;
n) Irrecoverable loss of sensitive information;
o) Any other activity requiring user intervention and occurring outside of the normal scope of system operation; and
p) Other significant or unusual events as deemed applicable by the regulatory body.

4.7.9 User Access Information

For each user account, the information to be maintained and backed up by the Event Wagering System must 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) Date and time account created;
e) The date and time of last log in;
f) Date of last password change;
g) Date and time account disabled/deactivated; and
h) Group membership of user account (if applicable).

4.8 Reporting Requirements

4.8.1 General Reporting Requirements

The Event Wagering System must 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 must apply for required reports:

a) The system must 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 must 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.

4.8.2 Operator Revenue Reports

The Event Wagering System must 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 cancelled;
e) Commission and fees collected (if applicable);
f) Event and market identifiers; and
g) Event status (in progress, complete, confirmed, etc.).

4.8.3 Operator Liability Reports

The Event Wagering System must 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.

4.8.4 Future Events Reports

The Event Wagering System must 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 cancelled on the gaming day (total and by wager); and
f) Event and market identifiers.

4.8.5 Significant Events and Alterations Reports

The Event Wagering System must be able to provide the following information needed to compile one or more reports for each significant event or alteration as applicable:

a) 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.

Appendix A: Operational Audit for Event Wagering Procedures and Practices

A.1 Introduction to Event Wagering Procedures and Practices

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, 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 must 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 must 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 must 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:

a) 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) 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 must 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 must be available to the player. During the registration process and when any terms and conditions are updated, the player shall agree to the terms and conditions. The terms and conditions must:

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 must be available to the player. During the registration process and when the privacy policy is updated, the player shall agree to the privacy policy. The privacy policy must 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, must 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 must be kept confidential, except where the release of that information is required by law.
b) There must 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 must 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 must be in place to satisfy the requirements for "Player Funds Maintenance" as

indicated within this document.

b) Positive player identification or authentication must 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) must be completed by the operator within a reasonable amount of time, unless there is a pending unresolved player complaint/dispute or investigation. Such investigation must 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 must 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 must 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 must only be possible to reduce the severity of self-imposed limitations upon 24 hours' notice, or as required by the regulatory body;
b) Players must be notified in advance of any operator-imposed limits and their effective dates. Once updated, operator-imposed limits must 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 must 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 must be a method for the operator to exclude a player from wagering as required by the regulatory body.

a) Players must 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 must 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 must 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 and potential winning wagers for the gaming day.

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 event 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 must 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 must be able to log complaints/disputes on a 24/7 basis.

b) Records of all correspondence relating to a complaint/dispute must be maintained for a period of five years or as otherwise specified by the regulatory body.
c) A documented process must 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 must be available to the player. The player protection information must 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.4.6 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 must be made available to a player for review prior to contest/tournament registration. The rules must include at a minimum:
    i. All conditions registered players must 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 must 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 must 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 must be recorded except for the number of entries, amount of entry fees and total prize pool.

A.5 Wagering Rules

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 must be approved by the regulatory body:

a) Wagering rules must be complete, unambiguous, and not misleading or unfair to the player.
b) Wagering rules that are presented aurally (via sound or voice) must also be displayed in written form.
c) Wagering rules must 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 must 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 General Rules Content

The following information must 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 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.

A.5.3 Wagering Information

In addition to the content of the previous section the following wagering information must be made available to the player.

a) 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;
b) Payout information, including possible winning positions, rankings, and achievements, along with their corresponding payouts, for any available wager option;
c) Any restrictive features of wagering, such as wager amounts or maximum win values;
d) A description on restricted players, including any applicable limitations on wagering for them (e.g. athletes shall not wager on their sport);
e) The procedures for handling incorrectly posted events, markets, odds/payouts, prices, wagers, or results;
f) A wager cancellation policy which must cater for wagers with multiple events (e.g., parlays) and indicate any prohibitions of cancellation (e.g., after a fixed time period);
g) 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;
h) 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;
i) 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;
j) 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;
k) 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);
l) The rules for any exotic wagering options (e.g., perfecta, trifecta, quinella, etc.) and the expected payouts;
m) 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;
n) How a winning wager is determined and the handling of an award in any case where a tie is possible;
o) 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 must clearly explain:
    i. Rounding up, down (truncation), true rounding; and
    ii. Rounding to what level (e.g., 5 cents).

A.5.4 In-Play Wagering

The player shall be informed in the wagering rules that due to varying communication speeds or broadcast transmission latencies:

a) Updates of the displayed information may put a player at a disadvantage to others who may have more up-to-date information; and
b) There may be delays Incorporated in the registered time of an in-play wager to prevent past-post wagers and cancellations.

A.5.5 Promotions and/or Bonuses

Players must 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 must be clear and unambiguous, especially where promotions or bonuses are limited to certain events, markets, or when other specific conditions apply.

A.5.6 Player Resources/Features

Where allowed by the regulatory body, the operator may provide resources/features 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 wagering rules must clearly describe the resources/features that are available, the advantage it offers (if any), and the options that exist for selection.
b) The wagering rules must disclose the method for obtaining each resource/feature. Any player resources/features that are offered to the player for purchase must clearly disclose the cost.
c) The availability and functionality of player resources/features must 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.

A.6 Wagering Procedures and Controls

A.6.1 Odds/Payouts and Prices

There must 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 must 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 must be maintained for a period of 90 days, or as otherwise specified by the regulatory body.

A.6.3 Suspending Markets or Events

There must 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 must 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 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 must provide a reason for cancellation to a player (e.g., past-post wager).

A.6.5 Wagering Periods

Documentation must 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 must be procedures in place for cases where access to the external feed is unavailable. There must 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 must 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 must provide a secure location for the placement, operation, and usage of wagering equipment, including Wagering Devices, displays, and communications equipment. Security policies and procedures must be in place and reviewed periodically to ensure that risks are identified, mitigated and underwritten by contingency plans. In addition:

a) Wagering equipment must be installed according to a defined plan and records of all installed wagering equipment must be maintained.
b) Wagering equipment must 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 must 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 must 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 must 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 must 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 must 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 must 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 must 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 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;
e) 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
f) 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 must 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

The operator, who offers remote wagering, or a third-party location service provider authorized by the regulatory body must, 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 to Technical Security Controls

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 must 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 transactions, 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 wagers and pays if a full recovery is not possible.

B.2.2 Physical Location of Servers

The Event Wagering System server(s) must 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) must:

a) Have sufficient protection against alteration, tampering or unauthorized access;
b) Be equipped with a surveillance system that must 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 must 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 must have their own individual authentication credential whose provision must be controlled through a formal process.
b) Authentication credential records must be maintained either manually or by systems that automatically record authentication changes and force authentication credential changes.
c) The storage of authentication credentials must be secure. If any authentication credentials are hard coded on a component of the system, they must be encrypted.
d) A fallback method for failed authentication (e.g., forgotten passwords) must be at least as strong as the primary method.
e) Lost or compromised authentication credentials and authentication credentials of terminated users must be deactivated, secured or destroyed as soon as reasonably possible.
f) The system must 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 must 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 must 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 must be recorded in a secure log.
i) The use of utility programs which can override application or operating system controls must 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 must implement the following user authorization requirements:

a) A secure and controlled mechanism must 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 must be documented and must be included in the review of access rights and privileges.
c) Any authorization information communicated by the system for identification purposes must be obtained at the time of the request from the system and not be stored on the system component.
d) The system must 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 must 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 must also be protected from the unauthorized execution of mobile code.

B.2.6 Verification Procedures

There must 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 must be gathered from the production environment through a process to be approved by the regulatory body.
b) The process must 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 must 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 must 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 must be recovered in the event of a disaster or equipment or software failure.
d) Any failure of verification of any component of the system must require a notification of the authentication failure being communicated to the operator and regulatory body as required.
e) There must 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, must be accounted for and have a nominated owner.

a) An inventory must be drawn up and maintained of all assets holding controlled items.
b) A procedure must exist for adding new assets and removing assets from service.
c) A policy must be included on the acceptable use of assets associated with the system and its operating environment.
d) Each asset must 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 must 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 must provide a logical means for securing the player and wagering data, including accounting, reporting, significant event, or other sensitive information, against alteration, tampering, or unauthorized access.

a) Appropriate data handling methods must 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 must be limited.
c) Encryption or password protection or equivalent security must 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 must 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 must 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 must 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 must be stored in areas of the server that are encrypted and secured from unauthorized access, both external and internal.
h) Production databases containing data must reside on networks separated from the servers hosting any user interfaces.
i) Data must be maintained at all times regardless of whether the server is being supplied with power.
j) Data must 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 must not be permitted without supervised access controls. In the event any data is changed, the following information must 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 must 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 and wagering data must be stored using reasonable protection methods. The Event Wagering System must be designed to protect the integrity of this data in the event of a failure. Redundant copies of this data must 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 must 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 must 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 must 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 must 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 must 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 must 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 must be possible to restore the system from the last backup point and fully recover. The contents of that backup must 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 must be provided with adequate primary power. Where the server is a stand-alone application, it must have an Uninterruptible Power Supply (UPS) connected and must have sufficient capacity to permit a graceful shut-down and that retains all player 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 must 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 must 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 must:

a) Address the method of storing player and wagering data to minimize loss. If asynchronous replication is used, the method for recovering data must be described or the potential loss of data must 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 must be permitted to establish communications between any system components. The Event Wagering System must 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 must be un-enrolled and disabled.

B.4.3 Communication Protocol

Each component of the Event Wagering System must function as indicated by a documented secure communication protocol.

a) All protocols must 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 must employ encryption and authentication.
c) Communication on the secure network must 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 must 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, must be secure by a means approved by the regulatory body. Player data, sensitive information, wagers, results, financial information, and player transaction information must 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, must 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 *GLI-26 Standards for Wireless Systems* must 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 must 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 must authenticate all users on the network and encrypt all network management communications.
b) The failure of any single item must not result in a denial of service.
c) An Intrusion Detection System/Intrusion Prevention System (IDS/IPS) must 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 must 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 must contain complete and comprehensive information about all wireless devices involved and must be able to be reconciled with all other networking devices within the site or venue.
e) Network Communication Equipment (NCE) must meet the following requirements:
   i. NCE must 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 must be physically secured from unauthorized access.
   iii. System communications via NCE must be logically secured from unauthorized access.
   iv. NCE with limited onboard storage must, 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 must be secured to prevent unauthorized access to the network. Unused services and non-essential ports must be either physically blocked or software disabled whenever possible.
g) In virtualized environments, redundant server instances may not run under the same hypervisor.
h) Stateless protocols, such as UDP (User Datagram Protocol), may 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) must be logged.
j) Virus scanners and/or detection programs must be installed on all systems. These programs must 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 must be capable of securely communicating with third-party service providers using encryption and strong authentication.
b) All login events involving third-party service providers must be recorded to an audit file.
c) Communication with third-party service providers must not interfere or degrade normal Event Wagering System functions.
   i. Third-party service provider data must not affect player communications.

ii. Connections to third-party service providers must not use the same network infrastructure as player connections.
iii. Wagering must be disabled on all network connections except for the player network;
iv. The system must not route data packets from third-party service providers directly to the player network and vice-versa
v. The system must not act as IP routers between player networks and third-party service providers.

d) All financial transactions must 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 must 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 must cover all relevant security requirements.
b) The services, reports and records provided by the third-party service providers must 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, must 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 must 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 must 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) must be restricted to authorized personnel.
d) Zone transfers to arbitrary hosts must be disallowed.
e) DNS Security Extensions (DNSSEC) must be in place.
f) Multi-factor authentication must be in place.
g) Registry lock must 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 must be developed and implemented.

a) Any player data and/or sensitive information must be encrypted if it traverses a network with a lower level of trust.
b) Data that is not required to be hidden but must be authenticated must use some form of message authentication technique.
c) Authentication must use a security certificate from an approved organization.
d) The grade of encryption used must be appropriate to the sensitivity of the data.
e) The use of encryption algorithms must be reviewed periodically to verify that the current encryption algorithms are secure.
f) Changes to encryption algorithms to correct weaknesses must be implemented as soon as practical. If no such changes are available, the algorithm must be replaced.
g) Encryption keys must 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 must follow defined processes established by the operator and/or regulatory body. These defined processes must 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 must only be allowed if authorized by the regulatory body and must:

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 must 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 must 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 must 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, must 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 must be located at the boundary of any two dissimilar security domains.
b) A device in the same broadcast domain as the system host must 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 must 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 must reject all connections except those that have been specifically approved.
g) The firewall must 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 must only allow remote access over the most up to date encrypted protocols.

B.7.5 Firewall Audit Logs

The firewall application must maintain an audit log and must disable all communications and generate an error if the audit log becomes full. The audit log must 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 must also be notified.

B.7.6 Firewall Rules Review

If required by the regulatory body, the firewall rules must be periodically reviewed to verify the operating condition of the firewall and the effectiveness of its security configuration and rule sets and must 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 must be adequate to ensure that only authorized versions of programs are implemented on the production environment. These change controls must 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 must follow defined processes established by the operator and/or regulatory body.

a) The production environment must 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 must be precluded from having access to promote code changes into the production environment.
c) There must be a documented method to verify that test software is not deployed to the production environment.
d) To prevent leakage of sensitive information, there must be a documented method to ensure that raw production data is not used in testing.
e) All documentation relating to software and application development must 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 must 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 must 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 must be carried out up to the highest level of access possible and must 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 must 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 must 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 must 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;
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 must 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 must be agreed between the CSP and the operator for all security requirements, and responsibilities for operation, management and reporting must 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. The ARP is a request and reply protocol and it is communicated within the boundaries of a single network, never routed across Internetwork nodes (connection points, either a redistribution point or an end point for data transmissions).

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.

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 event 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.

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 must take in response to various commands.

In-Play Wager – A wager that is placed while an event is in-progress or actually taking place.

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.

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 must 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 must 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 and wagering data, validation numbers, PINs, player data, passwords, secure seeds and keys, and other data that must 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.