GLI STANDARD SERIES

GLI-33:

STANDARDS FOR EVENT WAGERING SYSTEMS

VERSION: 2.0 DRAFT

REVISION DATE: JUNE 15, 2026

About This Standard

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

Operators and suppliers are expected to provide documentation, credentials, and associated access to source code and a production equivalent test environment with a request to the independent testing laboratory that it be evaluated in accordance with this technical standard. Upon the successful completion of testing, the independent testing laboratory will provide a report evidencing the evaluation of, or certification to, this standard.

GLI-33 should be viewed as a living document that will be tailored periodically to align with this developing industry over time as event 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 operators, developers, and suppliers. GLI has taken each of the standards documents and merged the unique rules, eliminated some rules and updated others, to reflect both the change in technology and the purpose of maintaining an objective standard that achieves common regulatory objectives without unnecessarily impeding technological innovation. It is the policy of GLI to update this document as often as warranted to reflect changes in technology and/or testing methods. This document will be distributed without charge and may be obtained by downloading it from the GLI website at www.gaminglabs.com or by contacting GLI at:

Gaming Laboratories International, LLC.
600 Airport Road
Lakewood, NJ 08701
Phone: (732) 942-3999
Fax: (732) 942-0043

1.1.3 Acknowledgment of Other Standards Reviewed

GLI acknowledges and thanks the regulatory bodies and other industry participants who have assembled rules, regulations, technical standards, and other documents which have been influential in the development of this document.

1.2 Purpose of Technical Standards

1.2.1 General Statement

The purpose of this technical standard is as follows:

a) To eliminate subjective criteria in the evaluation and/or certification of Event Wagering Systems.
b) To assess the criteria that impacts the credibility and integrity of event wagering from both revenue collection and player perspectives.
c) To establish a standard that will ensure event wagering is fair, secure, auditable, and able to be operated correctly.
d) To distinguish between local public policies and Independent Test Laboratory criteria,

acknowledging that it is the prerogative of each regulatory body to set its own public policies with respect to event wagering.

e) To recognize that the evaluation of internal control procedures (such as anti-money laundering, financial, and business processes) employed by operators should not be incorporated into the laboratory testing of the standard. Instead, these should be addressed within operational audits and assessments performed for local jurisdictions.
f) To develop a standard that can be easily revised to allow for new technology.
g) To formulate a standard that does not specify any particular design, method, or algorithm, thereby allowing a wide range of methods to conform to the standards while simultaneously encouraging the development of new methods.

1.2.2 No Limitation of Technology

One should be cautioned that this document shall not be read in such a way that limits the use of future technology. This document should not be interpreted to mean that if the technology is not mentioned, then it is not allowed. On the contrary, GLI will periodically review this standard and update it to include minimum standards for any new and relevant technology.

1.2.3 Adoption and Observance

This technical standard can be adopted in whole or in part by any regulatory body that wishes to implement a comprehensive set of technical requirements for Event Wagering Systems.

1.3 Other Documents That May Apply

1.3.1 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.

1.3.2 Minimum Internal Control Standards (MICS)

Implementing Event Wagering Systems is a complex endeavor, necessitating the development of internal processes and procedures to ensure that the gaming production environment is secure and controlled adequately. To that end, it is expected that a set of Minimum Internal Control Standards (MICS) will be established by the regulatory body to determine the minimum required internal processes for the management and handling of event wagering as well as the requirements for internal control of any system or component software and hardware within the gaming production environment, and their associated accounts. The regulatory body's MICS may also include technical security controls and testing requirements for the gaming production environment as well as change management policies.

1.3.3 Gaming Security Framework (GSF)

Adherence to the *GLI Gaming Security Framework (GLI-GSF)* is necessary for Event Wagering Systems. The GLI-GSF details technical security controls and testing requirements, which will be assessed during evaluations of the gaming production environment. This includes, but is not limited to, operational process reviews critical to compliance, vulnerability and penetration testing of the external and internal infrastructure and applications handling sensitive information, and any other criteria set by the regulatory body.

NOTE: The *GLI Gaming Security Framework (GLI-GSF)* is available free of charge at www.gaminglabs.com.

1.4 Interpretation of this Document

1.4.1 General Statement

This technical standard applies to systems that support wagering on sporting events or games, competitions, contests, matches, races, or other occurrences or type of activity 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 wagering events, markets, or wager types. The intent is to provide a framework to cover those currently known and permitted by law.

1.4.2 Operators and Software Suppliers

The components of an Event Wagering System, although they may be constructed in a modular fashion, are intended to function cohesively.

a) 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 gaming production environment shall be communicated to the independent test laboratory to facilitate creating a functionally equivalent test environment.
b) Because of the integrated nature of an Event Wagering System, there are several requirements in this document which may apply to both operators and software suppliers. In such cases, the collection of systems and solutions needed to meet these requirements will be considered to be the gaming production environment and the individual entities providing them will need to meet such eligibility requirements as the regulatory bodies deem appropriate for performance of these requirements.

NOTE: This document is not intended to determine which parties are responsible for meeting the requirements detailed herein. It is the responsibility of the stakeholders of each jurisdiction to determine how to best meet the requirements laid out in this document.

1.4.3 Use of "Mechanisms"

When a requirement in this technical standard requires that a "mechanism" be in place, it means that the operator or software supplier shall use a critical component or clear, documented process that has been effectively implemented to achieve the desired outcome. Operators and software suppliers

have the flexibility to determine what type of mechanism is best for the situation at hand, whether it is by the use of technology, an operational procedure, or a mix of activities. Compliance shall be evaluated based on the effectiveness of the overall mechanism rather than the use of any specific implementation approach.

1.5 Testing and Auditing

1.5.1 Laboratory Testing

The independent test laboratory will test and evaluate or certify the components of the Event Wagering System in accordance with the chapters of this technical standard within a controlled test environment, where applicable.

a) Unless otherwise directed by the regulatory body, the independent test laboratory shall be provided access to the component's source code along with the means to verify compilation of such source code. The result of the compiled source code shall be identical to that in the component submitted for evaluation or certification.
b) It may be necessary to perform additional laboratory testing when certain components are integrated with the Event Wagering System. This will be particularly relevant when the implementation involves changes to the component.
c) Where the regulatory body has adopted a change management program (CMP), such as the *GLI Change Management Program Guide (GLI-CMP)*, the CMP will be used to determine which changes to previously tested components require modification testing. The scope of any required modification testing will depend on the nature, extent, and potential impact of the changes.
d) Any requirements within the chapters of this technical standard which necessitate additional operational procedures to meet the intent of the requirement may be documented within the evaluation or certification report and used to supplement the scope of the operational audits and assessments.

1.5.2 Operational Audits and Assessments

The integrity and accuracy of the operation of an Event Wagering System is highly dependent upon operational procedures, configurations, and the gaming production environment's network infrastructure. As such, operational audits and assessments are essential additions to the testing and evaluation or certification of an Event Wagering System. Where required by the regulatory body, the following operational audits and assessments shall be performed on an annual basis, or at a frequency specified by the regulatory body:

a) An internal controls audit, against the applicable internal control procedures identified in Appendix A: Internal Control Procedures and Practices and the regulatory body's Minimum Internal Control Standards (MICS); and
b) An integrity and security assessment, against the applicable controls and tests identified in the GLI Gaming Security Framework (GLI-GSF) and any other controls and tests identified by the regulatory body.

Chapter 2: Platform/System Requirements

2.1 Introduction

2.1.1 General Statement

If the Event Wagering System is comprised of multiple computer systems at various sites, the system as a whole and all communication between its components shall conform to the applicable technical requirements within this document.

2.2 System Clock Requirements

2.2.1 System Clock

The Event Wagering System shall maintain an internal clock that reflects the current date and time that shall be used to provide for the following:

a) Time stamping of all transactions, configuration changes, and wagering events;
b) Time stamping of significant events; and
c) Reference clock for reporting.

2.2.2 Time Synchronization

The Event Wagering System shall implement a mechanism to ensure that all components that comprise the system operate on a common time reference sufficient to maintain the validity of time-based communications.

2.3 Control Program Requirements

2.3.1 Control Program Self-Verification

The Event Wagering System shall be capable of verifying that all critical control program components deployed on the system are authentic copies of the approved versions, using a software solution or other mechanism approved by the regulatory body. The critical control program verification function shall:

a) Perform self-verification of the critical control program components:
   i. At least once every twenty-four hours; and
   ii. Upon request by authorized personnel or the regulatory body;
b) Employ a cryptographically secure hash algorithm which produces a message digest of at least 128 bits. Other test methodologies shall be reviewed on a case-by-case basis;
c) Include all critical control program components which may affect event wagering operations, including but not limited to executables, libraries, wagering or system configurations, server-side wagering files, customized operating system files, components that directly control required system reporting, and database elements that directly affect system operations; and

d) Provide an indication of the verification failure if any critical control program component is determined to be invalid.

NOTE: To ensure full compliance, the critical control program verification function may need to be installed on each server hosting critical control program components that comprise the system, including all Player Account Managers and Wagering Platforms, if such functionality is not centralized to a single server.
NOTE: This requirement does not apply to Player Applications, including client-side graphics and audio files (e.g., wagering rules, help screens, etc.).

2.3.2 Control Program Independent Verification

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

2.4 Wagering Communications, Controls, and Overrides

2.4.1 Communication Loss

If communications between critical components of the Event Wagering System are lost, the affected components shall cease operations related to that communication. Detection of such communication failures may occur upon an attempted communication between components.

2.4.2 Wagering Management

The Event Wagering System shall be able to disable or suspend the following on demand, as applicable. A mechanism shall be in place to record the date and time for disabling or suspending and the reason for doing so:

a) All event wagering activity;
b) Individual wagering events and markets;
c) Individual bonusing/promotional offers;
d) Individual Retail Wagering Terminals; and
e) Individual Remote Player Device logins.

2.4.3 Wager Record Overrides

The Event Wagering System shall provide a mechanism for authorized personnel to settle, redeem, void, or cancel wagers. During each phase of the settlement, redemption, voiding, or cancellation process, the system shall update the wager status, the wager record history, and the player account balance accordingly.

2.5 Information to be Maintained

2.5.1 Information Retention

The Event Wagering System shall have mechanisms which:

a) Are capable of maintaining and backing up all applicable recorded information with timestamps and versioned data fields as discussed within this standard;
b) Where applicable, record bonusing/promotional amounts separately from other amounts (e.g., for wagers, wins or payouts, voids or cancellations, etc.); and
c) Can export this recorded information in machine-readable format for the purposes of analysis and auditing/verification (e.g., CSV, JSON, XLS, PDF, etc.).

NOTE: Internal control procedures may be in place to ensure this information is recorded where it is not maintained directly by the system.

2.5.2 Wager Record Information

The information to be maintained and backed up by the Event Wagering System for each individual wager placed by the player shall include, as applicable:

a) Unique wager record ID;
b) The date and time the wager was placed;
c) Each player choice involved in the wager:
    i. Unique wagering event ID and/or market ID, if different;
    ii. The description of the wagering event, market, and wager type (e.g., moneyline, point spreads, over/under, win/place/show, parlay, etc.);
    iii. Wager selection (e.g., athlete or team name and number) or combination of selections chosen, including selection names where practical;
d) Odds/payouts applicable at the time the wager was placed;
e) Total amount wagered;
f) Total amount paid or to be paid for settled or redeemed wagers;
g) Total amount voided or cancelled;
h) Rake, commission, or fees collected;
i) Any special conditions applying to the wager;
j) The results of the wager, if known, including whether the wager was settled through an early settlement feature;
k) Unique user account ID, unique terminal ID, or equivalent which issued the wager record;
l) For retail wagers:
    i. Wagering Venue Name/Site ID where issuance occurred;
    ii. Redemption period;
    iii. Open text field for attendant input of player description or picture file, if supported;
m) For a settled, redeemed, voided, or cancelled wager, if known:
    i. The date and time of settlement, redemption, voiding, or cancellation;
    ii. Unique user account ID, unique terminal ID, or equivalent which settled, redeemed, voided, or cancelled the wager record;
    iii. Wagering Venue Name/Site ID where settlement, redemption, voiding, or cancellation occurred;
n) Unique player account ID, or for anonymous wagers, method of payment (e.g., cash, personal check, cashier's check, wire transfer, money order, credit or debit instrument, electronic payment account, etc.);

o) Relevant location information (e.g., device ID, location data, connection type, etc.); and
p) The current status of the wager (e.g., pending, active, settled, redeemed, voided, cancelled, expired, etc.) and the date and time of each previous status change.

2.5.3 Wagering Event/Market Information

The information to be maintained and backed up by the Event Wagering System for each individual wagering event and market available for wagering shall include, as applicable:

a) Unique wagering event ID and/or market ID, if different;
b) The description of the wagering event, market, and wager type (e.g., moneyline, point spreads, over/under, win/place/show, parlay, etc.);
c) Available wager selections (e.g., athletes or team names and numbers) and amount wagered per wager selection;
d) The date and time the wagering period started or is scheduled to start, if known;
e) The date and time the wagering period ended or is expected to end, if known;
f) Total amount wagered;
g) Total amount paid for settled or redeemed wagers;
h) Total amount voided or cancelled;
i) Total rake, commission, or fees collected;
j) The date and time the wagering event occurred or is expected to occur, if known;
k) The wagering event and market outcome (e.g., winning wager selection);
l) The date and time that the wagering event and market outcome was confirmed, if known; and
m) The current status of the wagering event and market (e.g., pending, in progress, interrupted, voided, cancelled, confirmed, etc.) and the date and time of each previous status change.

2.5.4 Contest/Tournament Information

Where contests/tournaments are supported, the information to be maintained and backed up by the Event Wagering System for each contest/tournament shall include, as applicable:

a) Name or identification of the contest/tournament;
b) The participating wagering event IDs and/or market IDs, if different;
c) The date and time the contest/tournament occurred or is expected to occur, if known;
d) For each registered player:
    i. Unique player account ID and/or name;
    ii. Amount of entry fee collected, and the date and time collected;
    iii. Player scorings/rankings;
    iv. Amount of winnings paid, and the date and time paid;
e) Total amount of entry fees collected;
f) Total amount of winnings paid to players;
g) Total amount voided or cancelled;
h) Total rake, commission, or fees collected; and
i) The current status of the contest/tournament (e.g., pending, in progress, interrupted, voided, cancelled, complete, etc.) and the date and time of each previous status change.

2.5.5 Player Account Information

Where player account management is supported, the information to be maintained and backed up by the Event Wagering System for each player account shall include, as applicable:

a) Unique player account ID and username, if different;
b) The date and method from which the account was opened (e.g., remote vs. on-site), including relevant location information (e.g., device ID, location data, connection type, etc.);
c) The personally identifiable information (PII) collected by the operator to register a player and create the account, including, their full legal name, date of birth, residential address, contact information, and any other information required by the operator or the regulatory body;
d) The player's full or partial government identification number (e.g., driver's license number, social security number, taxpayer identification number, passport number, or equivalent), and their current and previous personal financial information (e.g., credit or debit instrument numbers, bank account numbers, etc.), which shall be encrypted or hashed to a cryptographic algorithm as allowed by the regulatory body;
e) The date and method of identity verification (e.g., automatic vs. manual), including:
    i. If a government identification credential is used for identity verification, a description of the government identification credential provided by the player to confirm their identity and its date of expiration;
    ii. If a government identification credential is not used for identity verification, the mechanism used to confirm the player's identity;
f) The date of player agreement to the operator's terms and conditions and privacy policies, including the versions agreed upon;
g) Previous accounts, if any, and reason for closure;
h) The account's current and previous authentication credentials, which shall be encrypted or hashed to a cryptographic algorithm as allowed by the regulatory body;
i) Account details and current account balance. All discretionary account funds shall be maintained separately;
j) The date and time the account is accessed by any person (player or operator), including relevant location information (e.g., device ID, location data, connection type, etc.) and duration of access;
k) Limitation/time-out/suspension information:
    i. The date and time of the request;
    ii. Description and reason of limitation/time-out/suspension;
    iii. The type of limitation/time-out/suspension (e.g., system-imposed weekly deposit limitation, one-hour time-out, self-imposed monthly deposit limitation, self-imposed temporary suspension, etc.);
    iv. The date and time limitation/time-out/suspension commenced;
    v. The date and time limitation/time-out/suspension ended or is scheduled to end, if known;
l) Financial Transaction information:
    i. Unique transaction ID;
    ii. The date and time of the transaction;
    iii. The type of transaction (e.g., deposit, withdrawal, adjustment, non-wager purchase, etc.);
    iv. Amount of transaction;
    v. Total account balance before/after transaction;
    vi. Total amount of fees paid for transaction, if any;
    vii. Unique user account ID or equivalent which handled the transaction;

viii. Method of deposit/withdrawal (e.g., cash, personal check, cashier's check, wire transfer, money order, credit or debit instrument, electronic payment account, etc.);
ix. Deposit authorization number or a unique identifier which can be used to authenticate the type of account and the source of the funds (i.e., source of where funds came from/went to);
x. Relevant location information (e.g., device ID, location data, connection type, etc.);
xi. The current status of the transaction (e.g., pending, in progress, interrupted, voided, cancelled, complete, etc.) and the date and time of each previous status change;

m) Player attribute information, if supported by the Event Wagering System:
i. If tied to a particular wagering event or market, unique wagering event ID and/or market ID, if different;
ii. The date and time of the transaction;
iii. Unique transaction ID;
iv. The criteria for the use of the player attribute (e.g., quantity of winning wagers, subscriptions, account memberships, player tracking information, wager requirements of the wagering event or market, etc.);
v. Type of action taken, or alteration made to the wager (e.g., wagering rule change, odds/payouts and prices change, or other configuration change related to the wager or wager result, etc.);
vi. The current status of the transaction (e.g., pending, in progress, interrupted, voided, cancelled, complete, etc.) and the date and time of each previous status change;

n) The date and method from which the account was closed (e.g., remote vs. on-site), including relevant location information (e.g., device ID, location data, connection type, etc.) and reason for closure; and
o) The current status of the player account (e.g., pending, active, inactive, closed, suspended, etc.) and the date and time of each previous status change.

2.5.6 Bonusing/Promotional Offer Information

Where bonusing/promotional offers are supported, the information to be maintained and backed up by the Event Wagering System for each bonusing/promotional offer shall include, as applicable:

a) Unique bonusing/promotional offer ID;
b) The participating wagering event IDs and/or market IDs, if different;
c) The date and time the bonusing/promotional offer was or is scheduled to be made active, if known;
d) The date and time the bonusing/promotional offer was or is scheduled to be retired, if known;
e) The bonusing/promotional offer parameters (e.g., value, eligibility, restrictions, order of precedence, etc.);
f) Current amount available for bonusing/promotional offer;
g) Total bonusing/promotional amounts issued;
h) Total bonusing/promotional amounts redeemed;
i) Total bonusing/promotional amounts expired;
j) Total bonusing/promotional offer adjustments; and
k) The current status of the bonusing/promotional offer (e.g., pending, active, disabled, retired, etc.) and the date and time of each previous status change.

2.5.7 Retail Wagering Terminal Information

Where retail wagering is supported, the information to be maintained and backed up by the Event Wagering System for each Retail Wagering Terminal shall include, as applicable:

a) Unique terminal ID or description (e.g., serial number, manufacturer, asset ID, etc.);
b) Wagering Venue Name/Site ID;
c) The type of terminal (e.g., OTC Wagering Terminal, Self-Service Wagering Terminal, etc.);
d) Terminal configuration data (e.g., peripherals, communications including IP Address, etc.);
e) Locally installed critical control programs;
f) For Self-Service Wagering Terminals:
    i. Significant event information;
    ii. Metering information;
g) For OTC Wagering Terminals:
    i. Unique user account ID or equivalent for the attendant session;
    ii. The date and time the attendant session began and ended;
    iii. The terminal balances at the start and end of the attendant session;
h) For each wager, wagering instrument, or financial transaction:
    i. Unique transaction ID;
    ii. The date and time of the transaction;
    iii. For wager transactions, the type of transaction (e.g., purchase, redemption, void, cancellation, etc.) and the unique wager record ID;
    iv. For wagering instrument transactions, the type of transaction (e.g., issuance, redemption, void, etc.) and the unique validation number;
    v. For financial transactions, the type of transaction (e.g., deposit, withdrawal, adjustment, non-wager purchase, etc.) and the unique player account ID;
    vi. Amount of transaction;
    vii. The current status of the transaction (e.g., pending, in progress, interrupted, voided, cancelled, complete, etc.) and the date and time of each previous status change;
i) The current status of the terminal (e.g., active, disabled, decommissioned, etc.) and the date and time of each previous status change.

2.5.8 System Significant Event Information

System significant event information to be maintained and backed up by the Event Wagering System shall include, as applicable:

a) Failed user account access attempts, including relevant location information (e.g., device ID, location data, connection type, etc.);
b) Program error or signature mismatch;
c) Significant periods of unavailability of any critical component of the system (e.g., any length of time wagering is halted for all players, communications are halted, and/or system functions cannot be successfully completed for any user);
d) Large wagers (single and aggregate over a specific time period) in excess of a value specified by the regulatory body, including wager record information;
e) Large wins or payouts (single and aggregate over a specific 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 to policies and parameters for operating systems, databases, networks, and applications (e.g., audit settings, password complexity settings, system security levels, manual updates to databases, etc.);
i) Changes to date/time on master time server;
j) Changes to the download data library, including the addition, changing, or deletion of software, where supported;
k) Changes to previously established criteria for a wagering event or market (not including line posting changes for active markets);
l) Changes to the outcome of a wagering event or market;
m) Changes to bonusing/promotional offer parameters (e.g., start/end, value, eligibility, restrictions, etc.) or change in status (e.g., presented, active, disabled, expired, etc.);
n) Player Account Management:
    i. Adjustments to a player account balance;
    ii. Changes made to sensitive information recorded in a player account (e.g., registration information, authentication credentials, payment methods, etc.);
    iii. Lock-out, time-out, suspension, or closure of a player account;
    iv. Large financial transactions (single and aggregate over a specific time period) in excess of a value specified by the regulatory body, including transaction information;
    v. Negative player account balance (due to adjustments and/or chargebacks);
o) Any incident or error that results in a loss of communication with, or other failure of, a third-party service provider's services that affects the system's operation (e.g. geolocation, know-your-customer, payment processing, statistics/line data, etc.);
p) Irrecoverable loss of sensitive information (permanent loss, corruption, or deletion of such information where restoration from backup or other recovery mechanisms is not possible);
q) Any other abnormal system events that require manual user intervention to restore normal operations, excluding routine or expected operational activities; and
r) Other significant or unusual events as deemed applicable by the regulatory body.

2.5.9 System Verification Information

System verification information to be maintained and backed up by the Event Wagering System for each critical control program component verification shall include, as applicable:

a) The data and time of the verification;
b) Critical control program component identification;
c) Expected control program component component's signature;
d) Generated control program component component's signature;
e) For on demand verifications, unique user account ID or equivalent executing the verification; and
f) Any other pertinent validation information (e.g., hash results and seeds used).

2.5.10 User Account Information

The information to be maintained and backed up by the Event Wagering System for each user account shall include, as applicable:

a) Unique user account ID and username, if different;
b) User's name and title or position;
c) Full list and description of functions that each group or user account may execute;
d) The date and time the account was created;
e) The date and time of each access, including relevant location information (e.g., device ID, location data, connection type, etc.);
f) The date and time of each authentication credential change;
g) The date and time the account was disabled or deactivated, including reason for status;
h) Group membership of user account; and
i) The current status of the user account (e.g., pending, active, inactive, disabled, deactivated, etc.) and the date and time of each previous status change.

2.6 Reporting Requirements

2.6.1 General Reporting Requirements

The Event Wagering System shall be capable of providing the necessary information to produce reports as required by the regulatory body. In addition to meeting the requirements in the section above for "Information Retention", the following requirements shall apply for required reports:

a) These required reports shall be able to be produced on demand, and for intervals required by the regulatory body (e.g., day-to-date (DTD), week-to-date (WTD), month-to-date (MTD), year-to-date (YTD), life-to-date (LTD), etc.).
b) Each required report shall contain:
   i. The operator's name (or other identifier), the title of report, the selected interval and the date/time the report was generated;
   ii. An indication of "No Activity" or similar message if no information appears for the period specified; and
   iii. Labeled fields which can be clearly understood in accordance with their function.
c) Where applicable, each required report shall separately indicate bonusing/promotional amounts from other amounts (e.g., for wagers, wins or payouts, voids or cancellations, etc.).

NOTE: In addition to the reports outlined in this section, the regulatory body may also require other reports utilizing the information stored under the "Information to be Maintained" section of this document.

2.6.2 Wagering Revenue Reports

The following information shall be provided by the Event Wagering System to produce one or more reports on wagering revenue for each wagering event as a whole and for each individual market within that wagering event, as applicable:

a) Unique wagering event ID and/or market ID, if different;
b) The description of the wagering event, market, and wager type (e.g., moneyline, point spreads, over/under, win/place/show, parlay, etc.);
c) The date and time the wagering event started and ended, if known;
d) Total amount wagered;
e) Total amount paid for settled or redeemed wagers;

f) Total amount voided or cancelled;
g) Total rake, commission, or fees collected;
h) The date and time that the wagering event and market outcome was confirmed, if different; and
i) The current status of the wagering event and market (e.g., pending, in progress, interrupted, voided, cancelled, confirmed, etc.) and the date and time of each previous status change.

2.6.3 Operator Liability Reports

The following information shall be provided by the Event Wagering System to produce one or more reports on operator liability, as applicable:

a) The starting liability amount (total amount held by the operator for player accounts), total additions and subtractions to account balances, and the ending liability amount;
b) The total amount of wagers placed on future wagering events;
c) The total amount of winnings or payouts owed but unpaid or partially paid by the operator on settled wagers; and
d) Any operational funds used to cover all other operator liability where required by the regulatory body.

2.6.4 Future Events/Markets Reports

The following information shall be provided by the Event Wagering System to produce one or more reports on each future wagering event or market for the gaming day, as applicable:

a) Unique wagering event ID and/or market ID, if different;
b) Total and by wager:
    i. Wagers placed prior to the gaming day for future wagering events and markets (e.g., wager placed yesterday, settles tomorrow);
    ii. Wagers placed on the gaming day for future wagering events and markets (e.g., wager placed today, settles tomorrow);
    iii. Wagers placed prior to the gaming day for wagering events and markets settling on the gaming day (e.g., wager placed yesterday, settles today);
    iv. Wagers placed on the gaming day for wagering events and markets settling on the gaming day (e.g., wager placed today. settles today); and
    v. Wagers voided or cancelled on the gaming day.

2.6.5 Player Account Activity Report

Where player account management is supported, the following information shall be provided by the Event Wagering System to produce one or more reports for each player account, as applicable:

a) Unique player account ID;
b) Beginning account balance;
c) Total amounts deposited;
d) Total amounts withdrawn;
e) Total amounts wagered;
f) Total amounts won or paid out;

g) Total amounts adjusted;
h) Total amounts for other additions to, or deductions from, the account balance; and
i) Ending account balance.

2.6.6 System Significant Events and Alterations Reports

The following information shall be provided by the Event Wagering System to produce one or more reports for each system significant event or alteration, as applicable:

a) The date and time of the significant event or alteration;
b) Event/component identification;
c) Identification of each individual who performed and/or authorized the significant event or alteration;
d) Reason/description of the significant event or alteration, including data or parameter altered;
e) Data or parameter value before alteration; and
f) Data or parameter value after alteration.

Chapter 3: Player Account Requirements

3.1 Introduction

3.1.1 General Statement

The requirements of this chapter apply to player accounts supported by the Event Wagering System and maintained by the operator. In addition to the requirements contained within this chapter, the operational procedures and controls indicated in the "Player Account Controls" section of this document shall also be met.

NOTE: Player accounts are required for a player to participate in remote wagering.

3.2 Player Account Registration and Verification

3.2.1 General Statement

The requirements of this section apply to registration, verification, validation, and/or activation of player accounts where such functionality is supported directly by the Player Account Manager.

3.2.2 Account Registration

Prior to the establishment of a player account, there shall be a method to collect player's personally identifiable information (PII) for the registration process.

a) At a minimum, the following registration information shall be collected from each player:
   i. Full name (i.e., first name and last name);
   ii. Date of birth (i.e., month, day, and year);
   iii. Contact information (i.e., email address and/or phone number);
   iv. Physical residential address (a post office box or equivalent is not acceptable); and
   v. Full or partial government identification number (e.g., driver's license number, social security number, taxpayer identification number, passport number, or equivalent); and
   vi. Any other information required by the operator or the regulatory body.
b) During the registration process, the player shall:
   i. Be denied registration if they submit a date of birth which indicates that they are underage;
   ii. If not all registration fields are required, be informed on the registration form which fields are required, which fields are optional, and the consequences of failing to complete any required fields;
   iii. Be provided with links to the terms and conditions for accessing and using the player account and the privacy policy governing the protection of PII, and acknowledge acceptance of both;
   iv. Acknowledge that they are prohibited from allowing any unauthorized person to access or use their player account;
   v. Consent to the monitoring and recording of the use of their player account by the operator and the regulatory body; and
   vi. Affirm that the PII the player is providing to open the player account is accurate.
c) A player may hold only one active player account at a time unless specifically authorized by the

regulatory body.

3.2.3 Identity Verification

The Player Account Manager shall employ a KYC Solution (Know-Your-Customer Solution) to reasonably prevent player account activation and access for persons who are underage, suspended, excluded, prohibited, or using false or unauthorized identity information. This solution may be provided in-house or by a third-party KYC Service Provider. The KYC Solution shall:

a) Use multisource verification, which may include governmental databases or other authoritative data sources, to verify the player's identity prior to account activation, unless otherwise specified by the regulatory body.
b) Verify the following player registration information as an exact match:
    i. Last name, except that partial matches may be used only to accommodate suffixes;
    ii. Date of birth; and
    iii. Full or partial government identification number (e.g., driver's license number, social security number, taxpayer identification number, passport number, or equivalent).
c) Verify the following player registration information as at least a partial match:
    i. First name, including common names or minor typographical differences; and
    ii. Physical residential address, including abbreviations, apartment or unit mismatches, or minor typographical differences.
d) If player identity cannot be automatically verified, apply one of the following manual verification mechanisms:
    i. Government identification credential verification;
    ii. Manual verification of the player registration information collected by the operator; or
    iii. Any other mechanism approved by the regulatory body.
e) Prevent any attempt to create an account by an individual who is identified to be:
    i. Underage or using the PII of a deceased person;
    ii. On any suspension lists maintained by the operator;
    iii. On any exclusion lists provided by the regulatory body; or
    iv. Prohibited from establishing or maintaining an account for any other reason.
f) Maintain details of identity verification in a secure manner.

3.2.4 Identity Validation

Where required by the regulatory body, the KYC Solution shall be designed to validate that the player creating the account is the legitimate owner of the claimed identity and to reasonably ensure the authenticity of any supporting evidence. The KYC Solution shall include at least one of the following, as applicable:

a) Requiring the player to correctly answer at least three dynamic knowledge-based questions derived from public and private data such as public records, credit reporting information, marketing data, and other recorded facts. The KYC Solution shall employ mechanisms to:
    i. Prevent duplicative questions from being presented to the same player during a single validation attempt;
    ii. Implement a limit on the number of incorrect answers a player is permitted to provide during a single validation attempt and ensure that a new and unique question is presented after any

incorrect response;
iii. Limit the amount of time a player is allotted to answer each question to no more than five minutes, or another period required by the regulatory body;
iv. Ensure that no question can be answered based on the player registration information already provided and/or information that is publicly available and easily accessible;

b) Matching Remote Player Device identification and contact information entered by the player during registration to the claimed identity. The KYC Solution shall employ mechanisms to:
i. Ensure that both the device used by the player to create the account and the contact information provided by the player during registration are associated with the claimed identity whose information has been verified;
ii. Reasonably detect device identification fraud or prior fraudulent activity associated with the device or contact information. If current or past fraudulent activity is detected, the KYC Solution shall determine whether device and contact information matching is sufficient to validate the player's claim to the identity and, if not, shall employ one of the other mechanisms set forth herein;

c) Requiring the player to submit a government identification credential that is reasonably determined to belong to the player. The KYC Solution shall employ mechanisms to:
i. Validate the authenticity and current validity of the credential and reasonably detect tampering, alteration, forgery, or reuse;
ii. Where biometric data or similar comparison technologies are used, employ measures such as a liveness check or equivalent safeguards to reasonably confirm that the credential belongs to the player presenting it;
iii. Prevent duplicate or repeated use of the same credential in a manner indicative of fraud, misuse, or account creation abuse;

d) Requiring the player to enter a One-Time Authentication Credential (OTAC) delivered through a validated communication channel associated with the claimed identity; or
e) Any other mechanism approved by the regulatory body in accordance with contemporary industry standards.

3.2.5 Mandatory Multi-Factor Authentication (MFA)

To maintain the security of accounts and reduce credential stuffing and account takeover attacks, multi-factor authentication (MFA) shall be enabled and configured by the player at the time the player creates the account. Once enabled and configured, MFA shall not be disabled by the player unless otherwise specified by the regulatory body. At least two of the following factors shall be used to achieve MFA:

a) Information known only to the player, such as a strong alphanumeric password, passphrase, or pattern, or answers to knowledge-based questions;
b) Something possessed by a player, such as a hardware token, software token, passkey, authenticator application, or OTAC;
c) A player's biometric data used in conjunction with a device-bound or otherwise securely managed authenticator, such as a fingerprint, facial recognition, voice recognition, or retina pattern scan; or
d) Any other factor approved by the regulatory body in accordance with contemporary industry standards.

NOTE: A single successful MFA may satisfy multiple concurrent or consecutive actions requiring MFA, provided such actions occur on the same Remote Player Device and within twenty-four hours or a period of time specified by the regulatory body. For example, a player may perform MFA upon account login and subsequently update their player registration information without being required to perform any additional MFA immediately thereafter.

3.2.6 Location Detection Permission

At the time of account creation, the Player Account Manager shall require location permission and record a geolocation check unless otherwise specified by the regulatory body. The player's location may be used to verify proximity to the declared physical residential address to permit account creation, provided all other identity verification and validation requirements are met.

3.2.7 Account Activation

The player account can only become active and begin to accept deposits and paid wagers once:

a) Identity verification and validation are successfully completed;
b) The player is determined to not be underage, deceased, on any suspension lists or exclusion lists, or prohibited from establishing or maintaining an account for any other reason;
c) The player has acknowledged the necessary terms and conditions and privacy policies; and
d) The player account registration process is complete.

NOTE: Additional identity verification and validation may be conducted throughout the lifetime of the player account if the operator has reasonable suspicion that the player's identity has been compromised.

3.3 Player Account Management

3.3.1 Authentication Credentials

A player account may be accessed at the Event Wagering System using authentication credentials, such as a username (or similar) and a strong alphanumeric password, a passkey, biometric data (e.g., facial recognition, fingerprints, or retina patterns), or a secure alternative means, for the player to perform authentication to log in. Allowable authentication credentials and 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 authentication credentials provided, an explanatory message shall be displayed which prompts the player to try again. The error message shall be the same regardless of which authentication credential is incorrect.
b) Where a player has forgotten their authentication credentials, MFA shall be employed for the retrieval or reset of their forgotten authentication credentials.
c) The player account shall be automatically locked-out after three consecutive failed access attempts in a thirty-minute period, or a period to be determined by the regulatory body. MFA shall be employed for the account to be unlocked. Alternatively, the system may, as supported, automatically release a locked-out account after thirty minutes, or a period to be determined by the regulatory body, have elapsed.

d) The system shall support a mechanism that allows for a player account to be locked-out or suspended by the operator in the event that suspicious player activity is detected. MFA shall be employed for the account to be unlocked.

3.3.2 Financial Transactions

Funds may be deposited to or withdrawn from the player account using payment methods allowed by the regulatory body which can produce a sufficient audit trail. Where financial transactions can be performed automatically by the Player Account Manager the following requirements shall be met:

a) The system shall provide confirmation/denial of every financial transaction initiated, including:
   i. The type of transaction (deposit/withdrawal);
   ii. The transaction value; and
   iii. For denied transactions, a descriptive message as to why the transaction did not complete as initiated.
b) Funds deposited into a player account shall not be available for wagering until they are received from the issuer or the issuer provides an authorization number indicating that the funds are authorized. The authorization number is to be maintained in an audit log.
c) Where financial transactions are allowed through Electronic Funds Transfers (EFT), there shall be security measures and controls to prevent EFT fraud. A failed EFT attempt may not be considered fraudulent if the player has successfully performed an EFT on a previous occasion with no outstanding chargebacks. Otherwise, the player account shall:
   i. Be temporarily locked-out for investigation of fraud after five consecutive failed EFT attempts within a ten-minute time period or a period to be determined by the regulatory body. If there is no evidence of fraud, the account may be unlocked; and
   ii. Have its access suspended after five additional consecutive failed EFT attempts within a ten-minute period or a period to be determined by the regulatory body and require MFA to recover the suspended account.
d) MFA shall be employed prior to completing large financial transactions (single and aggregate over a specific time period) in excess of a value specified by the regulatory body.
e) The system shall employ a mechanism that can detect and prevent any withdrawal activity initiated by a player that would result in a negative account balance. Where payment processing issues outside the control of the system cause an account to be overdrawn, the player account shall be suspended until the negative account balance is settled.
f) Unless otherwise specified by the regulatory body, withdrawals from a player account shall be paid directly to an electronic payment account in the name of the player or made payable to the player and forwarded to the player's residential address using a secure delivery service or through another payment method that is not prohibited by the regulatory body. The name and residential address are to be the same as held in player registration details.
g) If a player initiates a financial transaction and that transaction would exceed limits put in place by the operator and/or regulatory body, this transaction may only be processed provided that the player is clearly notified that they have withdrawn or deposited less than requested.
h) It shall not be possible to transfer funds between two player accounts.
i) Security or authorization mechanisms shall be in place to ensure that only authorized adjustments can be made to player account balances, and these changes are auditable.

NOTE: To support use of a single player account across multiple jurisdictions, it is recommended that the

system maintain separate wallets to handle funds deposited through various payment methods. This is to address cases where one jurisdiction prohibits a payment method that another jurisdiction permits.

3.3.3 Transaction Log or Account Statement

The Player Account Manager shall be able to provide a transaction log or account statement history to a player upon request. The information provided shall include sufficient information to allow the player to reconcile the statement or log against their own financial records. Information to be provided shall include, at a minimum, details on the following types of transactions within the past year or other time period as requested by the player or as required by the regulatory body, as applicable:

a) Financial transactions (transaction time stamped with a unique transaction ID):
   i. Deposits to the player account;
   ii. Withdrawals from the player account;
   iii. Bonusing/promotional amounts added to/removed from the player account (outside of wagers);
   iv. Manual adjustments or modifications to the player account (e.g., due to refunds);
   v. Any non-wager purchases;
b) Wager transactions (placement/settlement/redemption time stamped with a unique wager record ID):
   i. The description of the wagering event, market, and wager type (e.g., moneyline, point spreads, over/under, win/place/show, parlay, etc.);
   ii. Total amount wagered;
   iii. Total amount paid for settled or redeemed wagers;
   iv. Total bonusing/promotional amounts wagered/awarded;
   v. Total amount voided or cancelled;
   vi. Rake, commissions, or fees collected;
   vii. The complete wager information as indicated in "Wager Record" section of this document for wagers whose results have yet to be determined and wagers which were settled or redeemed within the last fourteen days, or a period specified by the regulatory body; and
c) Any other additions to, or deductions from, the account balance that would not otherwise be metered under any of the above-listed items.

NOTE: Where supported by the system, the player's self-imposed limitation, time-out, and suspension history may also be included.

3.3.4 Account Updates

MFA shall be employed for a player to access and update their registration information and authentication credentials, and to add, modify, or remove the payment methods used for financial transactions as supported by the Player Account Manager. In addition, there shall be a mechanism for the operator to perform these updates on behalf of a player upon request or where necessary. If any required registration information is re-entered or modified, the accuracy of the re-entered or modified registration information shall be verified before the player is allowed to conduct any further wagers or financial transactions.

3.3.5 Account Closure

Players shall be provided with a mechanism to close their player account at any time unless the operator has suspended the player account for reasons in which would prevent account closure. In addition, there shall be a mechanism for the operator to close a player account.

a) MFA shall be employed by the player to initiate an account closure request.
b) The player account closure process shall commence immediately upon receipt of the account closure request and result in the account being closed after:
   i. All active wagers have been settled, redeemed, voided, or cancelled; and
   ii. Any unrestricted player funds remaining in a player account have been refunded to the player, provided that the operator acknowledges that the funds have cleared.
c) A player shall not be encouraged or induced to keep their player account open following their account closure request to close their account. However, an operator may explain the effects of an account closure and ask the player if they wish to proceed.

3.3.6 Inactive Player Accounts

The Player Account Manager shall have a mechanism for the operator to identify, manage, and close inactive player accounts. Any unrestricted player funds remaining in a closed inactive player account shall be refunded or otherwise handled in accordance with the operator's internal control procedures.

3.4 Limitations, Time-Outs, and Suspensions

3.4.1 General Statement

The requirements in this section apply where the Player Account Manager supports the ability to directly manage and implement responsible gaming tools, including limitations, time-outs, and/or suspensions.

3.4.2 Limitations

Players shall be provided at all times with a mechanism to impose limitations for account activity including but not limited to deposits and wagers over a player-specified time period (e.g., day, week, month) as required by the regulatory body. In addition, there shall be a mechanism for the operator to impose limitations for account activity as required by the regulatory body.

a) Once established by a player and implemented by the system, it shall only be possible to reduce the severity of self-imposed limitations after the time period of the previous limit has expired, or as required by the regulatory body.
b) Players shall be notified in advance of any system-imposed limits and their effective dates. Once updated, system-imposed limits shall be consistent with what is disclosed to the player.
c) Upon receiving any self-imposed or system-imposed limitation order, the system shall ensure that all specified limits are correctly implemented immediately or at the point in time (e.g., next login, next day) clearly indicated to the player.
d) The self-imposed limitations set by a player shall not override more restrictive system-imposed

limitations. The more restrictive limitations shall take priority.

e) Limitations shall not be compromised by internal status events, such as time-outs or self-imposed suspension orders and revocations.

3.4.3 Time-Outs

Players shall be provided at all times with a mechanism to establish a player-specified time-out period up to seventy-two hours, or a period specified by the regulatory body. In addition, there shall be a mechanism for the operator to impose a time-out period on a player. During a time-out period:

a) The player may not place new wagers or deposit funds to their player account.
b) The player shall not be prevented from withdrawing any or all of their unrestricted player funds, provided that the operator acknowledges that the funds have cleared.

3.4.4 Suspensions

Players shall be provided at all times with a mechanism to suspend their player account for a player-specified time period (no less than seventy-two hours, or a period specified by the regulatory body) or indefinitely, as required by the regulatory body. In addition, there shall be a mechanism for the operator to suspend a player account as required by the regulatory body. While a player account is suspended:

a) The player shall be given a notification containing suspension status that the account is suspended, the reason for suspension, the restrictions placed on the account, and general instructions for resolution where possible.
b) The player shall be prevented from:
   i. Placing new wagers;
   ii. Depositing funds to their player account with the exception of settling a negative account balance, but only to the extent the account balance is brought back to zero; and
   iii. Making changes to or closing their player account, unless authorized by the operator.
c) The player shall not be prevented from withdrawing any or all of their unrestricted player funds, provided that the operator acknowledges that the funds have cleared, and that the reason for suspension would not prohibit a withdrawal.

3.5 Bonusing/Promotional Offers

3.5.1 General Statement

Bonusing/promotional offers, that are redeemable for cash, wagering credits, or merchandise, may be provided to a player based upon pre-determined events or criteria established by the parameters of the offers.

3.5.2 Player Cancellation of Offer Participation

The player shall be provided with a mechanism to cancel participation in a bonusing/promotional offer that utilizes restricted bonusing/promotional credits. In addition, there shall be a mechanism

for the operator to perform cancel participation on behalf of a player upon request or where necessary.

a) Upon request for cancellation, the player shall be informed of the amount of unrestricted player funds that will be returned upon cancellation and the value of restricted bonusing/promotional credits that will be removed from the player account.
b) If the player elects to proceed with cancellation, unrestricted player funds remaining in a player account shall be returned in accordance with the terms of the offer.

3.5.3 Player Completion of Offer Terms

Once a player has met the terms of a bonusing/promotional offer, the winnings earned while participating in the offer shall not be limited (i.e., the restricted bonusing/promotional credits of the offer will become unrestricted bonusing/promotional credits).

Chapter 4: Remote Player Device and Application Requirements

4.1 Introduction

4.1.1 General Statement

The requirements of this chapter apply to the Remote Player Devices and Player Applications used by the player to remotely take part in wagers and financial transactions with the Event Wagering System over a public network or private network, depending on the implementations authorized by the regulatory body.

4.2 Player Applications

4.2.1 General Statement

A Remote Player Device interacts with the Event Wagering System through a Player Application, which may be downloaded to or installed on the device (mobile application or desktop application), accessed through the device's browser interface (web application), or implemented through a combination of these methods.

4.2.2 Application Identification

Player Applications shall contain sufficient information to identify the application and its version, which, for example, may be displayed via a display screen or contained in the application source code.

4.2.3 Application Validation

For Player Applications installed locally on the Remote Player Device, it shall be possible to validate that the application is an authorized and suitable version for use with the Event Wagering System.

NOTE: Application validation methods 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.
NOTE: This requirement does not apply to client-side graphics and audio files (e.g., wagering rules, help screens, etc.).

4.2.4 Compatibility Verification

During any installation or initialization and prior to commencing event wagering operations, the Player Application used in conjunction with the Event Wagering System shall detect any incompatibilities or resource limitations with the Remote Player Device that would prevent proper operation of the application (e.g., software version, minimum specifications not met, browser type, browser version, plug-in version, etc.).

4.2.5 Communications

The Player Application shall be designed or programmed such that it may only communicate with authorized critical components through secure communications.

4.2.6 Application Errors

If Player Application validation fails, device compatibility requirements are not met, resource limitations prevent proper operation, or communication between the Event Wagering System and the Remote Player Device is lost, the application shall prevent event wagering operations and provide indication of an error. It is permissible for the application to detect such conditions when the application or device attempts to communicate with the system.

4.2.7 Client-Server Interactions

The following requirements apply to Player Applications and the client-server interactions between the Remote Player Device and Event Wagering System:

a) Players shall not be able to use the application 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 application shall not automatically disable any virus scanners and/or detection programs or alter any device-specified firewall rules to open ports that are blocked by either a hardware or software firewall;
c) The application shall not access any TCP/UDP ports (either automatically or by prompting the user to manually access) which are not necessary for the communication between the Remote Player Device and the server;
d) If the application includes additional non-wagering related functionality, this additional functionality shall not alter the application's integrity in any way;
e) The application shall not possess the ability to override the volume settings of the Remote Player Device; and
f) The application shall not store sensitive information in an unprotected manner. It is recommended that autocomplete, password caching, or other methods that automatically populate password fields be disabled by default for the application.

4.2.8 Application Content

Player Applications shall not contain any malicious code or functionality deemed to be malicious in nature by the regulatory body. This includes, but is not limited to, unauthorized file extraction/transfers, unauthorized device modifications, unauthorized access to any camera, microphone, or player location, unauthorized access to any locally stored personal information (e.g., contacts, calendar, etc.), and malware.

4.2.9 Cookies

Where cookies are used, the player shall be informed of the cookie use upon Player Application access or during player registration. When cookies are required for event wagering, wagering cannot occur if they are not accepted by the Remote Player Device. All cookies used shall contain no malicious code.

4.3 Player Access

4.3.1 Account-Based Wagering

A player may only place a wager on a Remote Player Device by using funds from their player account (i.e., anonymous wagers are prohibited).

4.3.2 Multi-Factor Authentication (MFA) for Login

Multi-Factor Authentication (MFA) shall be performed upon each login attempt from a specific Remote Player Device and shall be successfully completed before initial access to the player account is granted. After a player successfully logs into their account on that device using MFA, the Event Wagering System may allow the player to designate that account-device pairing as trusted for a period not to exceed fourteen days, or another period specified by the regulatory body. During this period:

a) Only re-authentication for the same account-device pairing may be exempted from MFA, provided the account-device pairing maintains its trusted status.
b) Any attempt to re-authenticate to a different player account from the same device or the same account from a different device shall undergo MFA and once that is successfully completed, the new account-device pairing may be exempted from MFA, subject to all of the conditions prescribed herein.
c) If the account-device pairing maintains its trusted status, the system shall require MFA to re-establish this status.

4.3.3 Post-Login Information

Once a player is successfully logged in, the Player Application shall make the following available to the player:

a) Any material updates to the terms and conditions and/or privacy policies (i.e., beyond any grammatical or other minor changes) which shall be agreed upon by the player prior to allowing further access to their player account.
b) The last date and time the player logged into their player account.
c) Current account balance information, including any bonusing/promotional credits, and transaction options. All discretionary account funds, including restricted bonusing/promotional credits and bonusing/promotional credits that have a possible expiration shall be indicated separately.

4.3.4 Information Access

In addition to the "Wagering Requirements" within this document, the Player Application shall be able to provide access to the required "Operator Display Content", either directly from the player interface or from a page accessible to the player, including, but not limited to pages containing:

a) Wagering Rules;
b) Player Protection Information;
c) Terms and Conditions; and
d) Privacy Policies.

NOTE: During laboratory testing, the independent test laboratory shall ensure that the Player Application provides access to placeholder pages on which the operator will be responsible to disclose the required "Operator Display Content".

4.3.5 Access Inactivity

After thirty minutes of inactivity while logged into their player account on a Remote Player Device, or a period determined by the regulatory body, the player shall be required to re-authenticate to access their player account on that device. No further wagers or financial transactions on that device are permitted until the player has been re-authenticated.

NOTE: Where the system provides one-way communication or content streaming and the player's expected interaction is passive, such as viewing the transmission of a wagering event, the absence of player input shall not, by itself, cause the player to be treated as inactive, unless otherwise specified by the regulatory body.

4.4 Device and Application Integrity, Monitoring, and Security

4.4.1 Device Identification

The Event Wagering System shall generate a persistent, tamper-resistant identifier for each Remote Player Device.

4.4.2 Multiple Devices or Accounts

To reduce the risk that Remote Player Devices or player accounts are used in a fraudulent manner, the Event Wagering System shall employ reasonable mechanisms to monitor the device used by a player to access their player account and, at a minimum, shall detect and perform all necessary due diligence or flag for investigation when:

a) More than four unique accounts are accessed from the same device within a fourteen-day period, or other period specified by the regulatory body; and
b) More than three unique devices are accessed by the same account within a twenty-four-hour, or other period specified by the regulatory body.

NOTE: This requirement does not preclude an operator from performing other procedures designed to detect and prevent suspicious player activity or other fraudulent activity, nor does it preclude an operator from conducting multiple device investigations based on narrower or more restrictive parameters (e.g., fewer devices or a shorter timeframe).

4.4.3 Device and Application Integrity and Attestation

The Event Wagering System shall verify that Remote Player Devices, Player Applications, and related data are authentic, untampered, and operating under secure runtime conditions. The system shall employ multiple detection methods to reasonably identify non-secure devices that may affect the integrity of the device or application, which may include compromised runtime environments, application-level tampering, system-level tampering, code hooking, rooting, jailbreaking, emulators,

virtualization, or similar conditions. These detection methods may include controls that function independently of native operating system security or attestation services.

4.4.4 Application Runtime Protection

The Event Wagering System shall continuously monitor the Player Application during execution to:

a) Reasonably detect unauthorized interference, which may include code injection, overlay attacks, memory tampering, manipulation of security functions, interference with application functionality, unauthorized modification of Application Programming Interface (API) calls, or similar activity; and
b) Take reasonable action upon detection to prevent compromise, which may include logging out the player, restricting functionality, denying wagering while the interference is present, and/or generating alerts for investigation.

4.5 Geolocation Operations and Enforcement

4.5.1 Geolocation Solution Requirements

Where required by the regulatory body, the Event Wagering System shall employ a Geolocation Solution to perform geolocation checks to authenticate a Remote Player Device's location data. This solution may be provided in-house or by a third-party Geolocation Service Provider. In addition to the requirements contained within this chapter, the operational procedures and controls indicated in the "Geolocation Solution Controls" section of this document shall also be met.

NOTE: Where remote wagering occurs over a private network, the Event Wagering System may use a location detection component in lieu of a Geolocation Solution, provided the component reasonably detects in real time when a player is no longer within the permitted geofence and responds as required by the regulatory body. Such methods may include beacon technology, directional antennas, or other technologies evaluated on a case-by-case basis by the independent test laboratory or regulatory body.

4.5.2 Geolocation Triggering Actions

The Event Wagering System and/or Geolocation Solution shall identify the triggering actions that require a geolocation check before the action is accepted or completed, as required by the regulatory body. To identify the player's location, a geolocation check shall be required prior to:

a) Accepting a paid wager where any of the following conditions apply:
   i. The player is attempting to place the first paid wager after logging in on a specific Remote Player Device;
   ii. No successful geolocation check has occurred within the preceding twenty minutes, or other recheck frequency specified by the regulatory body; or
   iii. A change to the player's IP Address has been detected.
b) Completing the following account management activities:
   i. Account creation;
   ii. Large financial transactions (single and aggregate over a specific time period) in excess of a value specified by the regulatory body; and

iii. Changes made to sensitive information recorded in a player account (e.g., registration information, authentication credentials, payment methods, etc.).

NOTE: As required by the regulatory body, the recheck frequency for mobile connections may increase based on the player's proximity to the border of the permitted geofence, using an assumed travel velocity of sixty-five miles per hour (one hundred and five kilometers per hour), or another velocity specified by the regulatory body.

4.5.3 Geolocation Checks, Logging, and Failures

For each geolocation check, the Event Wagering System shall communicate a geolocation request to the Geolocation Solution using an anonymized identifier for the player. This anonymized player ID shall not include any names or other PII (e.g., a player account ID is acceptable). The Event Wagering System shall maintain sufficient records to associate the geolocation check with the applicable player and device.

a) Each geolocation check and its result shall be recorded in a log, which shall include, at a minimum, the anonymized player ID, date and time of the check, relevant location information (e.g., device ID, location data, connection type, etc.), and geolocation result including the reason for any geolocation failure.
b) A geolocation failure occurs when, at the time of a required geolocation check:
   i. The device's location data cannot be authenticated by the Geolocation Solution (e.g., not enough location data or data accuracy is low);
   ii. The device's required location services, permissions, settings, configurations, or other conditions necessary for reliable geolocation are disabled, unavailable, unreliable, unsupported, or manipulated;
   iii. The Geolocation Solution detects fraud, tampering, spoofing, proxying, or other conditions that may prevent reliable authentication of the player's real-world geographic location; or
   iv. The regulatory body requires the triggering action to occur only within a permitted geofence, and the device's physical location is determined by the Geolocation Solution to be outside the permitted geofence.
c) Upon detection of a geolocation failure, the Event Wagering System shall:
   i. Reject the attempted triggering action;
   ii. Notify the player that the attempted triggering action could not be accepted or completed due to a geolocation failure; and
   iii. Prevent the triggering action from being accepted or completed until the geolocation failure is resolved by a subsequent successful geolocation check.

4.5.4 Geolocation Data Sources and Cross-Validation

The Event Wagering System and/or Geolocation Solution shall use authenticated location data from the Remote Player Device to determine the device's real-world geographic location. To reasonably ensure the device's location data is accurate and reliable, the Event Wagering System and/or Geolocation Solution shall:

a) Cross-validate the device's location data against multiple independent location data sources, where available and applicable, to reasonably determine the real-world geographic location of the player, including, but not limited to:

i. IP Address analysis;
ii. Global Positioning System (GPS) or Global Navigation Satellite System (GNSS);
iii. Wi-Fi and cellular triangulation; and
iv. Device sensor data, where applicable.

b) Not utilize an IP Address analysis as a primary location data source for geolocation checks unless otherwise authorized by the regulatory body. An IP Address analysis may be used as a supporting location data source to identify network-based location risks, which may include TOR exit nodes, data center proxies, residential proxies, proxy services, anonymizers, unauthorized VPN usage, and similar technologies.

NOTE: The use of a Virtual Private Network (VPN) may be permitted only where location data other than IP Address can reliably confirm the real-world geographic location of the player.

4.5.5 Geolocation Spoofing, Proxying, and Evasion Detection

The Event Wagering System and/or Geolocation Solution shall reasonably detect and prevent the use of technologies, services, or methods intended to conceal, relay, proxy, spoof, falsify, or otherwise misrepresent a player's real-world geographic location. Such methods include, at a minimum:

a) Network-routing techniques that may conceal, relay, proxy, or misrepresent the player's real-world geographic location;
b) Fake location applications, spoofing tools, manipulated location services, or other location-data falsification methods;
c) Remote desktop software, remote control tools, screen-sharing tools, or similar relay technologies;
d) Emulators, virtualization tools, or other software used to circumvent or falsify geolocation controls; and
e) Other technologies or techniques intended to interfere with, bypass, or falsify geolocation results.

4.5.6 Geolocation Integrity Risks

The Event Wagering System and/or Geolocation Solution shall implement best practice security mechanisms to reasonably detect and prevent geolocation integrity risks.

4.5.7 Geolocation Beacon Technology

When Beacon Technology is used by the Event Wagering System and Geolocation Solution to assist in enforcing the permitted geofence, such as short-range communications technology:

a) The Beacon Technology shall support configuration and adjustment of signal strength, broadcast range, and related parameters to establish and maintain the permitted geofence as accurately as reasonably practicable; and
b) The tokens broadcast by the Beacon Technology shall be refreshed at least every five minutes, or a period otherwise specified by the regulatory body. Expired tokens shall be invalidated so as to prevent attacks or hacking.

NOTE: Alternative methodologies and technologies of location detection shall be reviewed and approved by the regulatory body on a case-by-case basis.

Chapter 5: Retail Wagering Terminal Requirements

5.1 Introduction

5.1.1 General Statement

The requirements of this chapter apply to the Retail Wagering Terminals used by the player to take part in wagers and financial transactions with the Event Wagering System within a Wagering Venue. A wager may be placed within a Wagering Venue using one of the following types of Retail Wagering Terminals as allowed by the regulatory body. Any other types of Retail Wagering Terminals will be reviewed on a case-by-case basis, as allowed by the regulatory body.

a) Self-Service Wagering Terminal: A kiosk or other equipment 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 wager records and other authorized activities.
b) Over-the-Counter (OTC) Wagering Terminal: A workstation or other equipment that at a minimum will be used by an attendant for the execution or formalization of wagers placed on behalf of a player and, if supported, may be used for redemption of wager records and other authorized activities.

NOTE: For operators who offer retail wagering using attendant-controlled Remote Player Devices within a Wagering Venue, the "Remote Player Device and Application Requirements" shall be required.

5.2 Self-Service Wagering Terminals

5.2.1 General Statement

A player places a wager at a Self-Service Wagering Terminal by using funds from their player account or by using peripheral devices as authorized by the regulatory body.

5.2.2 Kiosks as Self-Service Wagering Terminals

All proprietary components of the Self-Service Wagering Terminal shall meet the applicable "Kiosk Terminal Requirements" and "Kiosk Software Requirements" established within the *GLI-20 Standards for Kiosks* and other applicable technical requirements observed by the regulatory body.

5.2.3 Gaming Devices as Self-Service Wagering Terminals

Where Gaming Devices acting as Self-Service Wagering Terminals are permitted by the regulatory body, their proprietary components are not required to meet the requirements for Kiosks provided they meet the applicable "Gaming Device/Machine Requirements" established within the *GLI-11 Standards for Gaming Devices* and/or other applicable technical requirements observed by the regulatory body.

5.3 OTC Wagering Terminals

5.3.1 General Statement

A player places a wager at OTC Wagering Terminal by using funds from their player account or by providing payment for the wager directly to the attendant.

5.3.2 Attendant Interface Requirements

The attendant interface is an interface application or program through which the attendant views and/or interacts with the OTC Wagering Terminal. The attendant interface shall meet the applicable "Player Interface Requirements" within this document.

NOTE: Access through the attendant interface shall meet the applicable "Workstation Access Controls" described within this document.

5.3.3 Touch Screen Displays

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

5.3.4 OTC Printer Requirements

If the OTC Wagering Terminal connects to a printer to produce printed wager records and/or wagering instruments, the printer and/or OTC Wagering Terminal shall be able to detect and indicate the following error conditions, where supported. It is permissible for the error condition to be detected when it tries to print:

a) Low battery (where power is external to the OTC Wagering Terminal);
b) Out of paper/paper low; and
c) Printer disconnected.

5.3.5 OTC Wager Record Handling

OTC Wagering Terminals used to settle, redeem, void, or cancel wagers shall meet the following technical requirements:

a) When wager records are presented for settlement, redemption, voiding, or cancellation at an OTC Wagering Terminal, the attendant shall scan the barcode (via a barcode reader or equivalent) or manually input the wager record ID and perform a verification with the Event Wagering System.
b) The Event Wagering System shall have the ability to identify and provide a notification to the OTC Wagering Terminal in the case of an invalid or unredeemable wager record for the following conditions:
    i. Wagering event has concluded and the wager record is not a winner;
    ii. Early settlement, voiding, or cancellation is unavailable;
    iii. Wager record cannot be found on file or has expired;
    iv. Wager record has already been settled, redeemed, voided, or cancelled; or

v. The value of wager record differs from amount on file. This requirement can be met by display of wager record for confirmation by the OTC Wagering Terminal during the settlement, redemption, voiding, or cancellation process.

c) The OTC Wagering Terminal may issue a settlement, redemption, voiding, or cancellation receipt. If printed, the settlement, redemption, voiding, or cancellation receipt, at a minimum, shall contain the following information, as applicable:
   i. Unique user account ID, unique terminal ID, or equivalent which issued the wager record;
   ii. Unique wager record ID;
   iii. The date and time of settlement, redemption, voiding, or cancellation;
   iv. Total amount settled, redeemed, voided, or cancelled; and
   v. Unique user account ID, unique terminal ID, or equivalent which settled, redeemed, voided, or cancelled the wager record.

5.3.6 Wireless OTC Wagering Terminals

For wireless OTC Wagering Terminals, the applicable requirements for "Player Applications" of the previous chapter shall also be met. Additionally, communication shall only occur between the wireless OTC Wagering Terminal and the Event Wagering System via authorized access points within the Wagering Venue.

5.4 Retail Wagering Terminal Management

5.4.1 Retail Wagering Terminal Monitoring

The Event Wagering System shall be equipped to correctly process transactions, read and store the applicable significant events and transaction information, and specific meter values from the Retail Wagering Terminals, through secure communications.

5.4.2 Terminal Identification

The Event Wagering System shall uniquely identify each connected Retail Wagering Terminal. This unique identification number shall be utilized by the Event Wagering System to log and track all essential information pertaining to the corresponding Retail Wagering Terminal. Furthermore, the system shall prevent the duplication of these identification numbers to ensure the integrity and accuracy of the terminal tracking.

5.4.3 Integrity of Protocol Communications

The Retail Wagering Terminal shall be designed or programmed such that it may only communicate with authorized critical components through secure communications. If communication between the Event Wagering System and the Retail Wagering Terminal is lost, the terminal shall prevent further wagering operations and display an appropriate error message. It is permissible for the software to detect this error when the terminal tries to communicate with the system.

5.4.4 Terminal Transaction Requirements

The Event Wagering System and Retail Wagering Terminals may support the use of wagering instruments (vouchers and coupons) and/or cashless wagering, provided such transactions shall be processed accurately through secure communications. In addition, as applicable:

a) The issuance and/or redemption of wagering instruments shall meet the applicable "Validation System Requirements" of the *GLI-13 Standards for Monitoring and Control Systems and Validation Systems* and/or other applicable technical requirements observed by the regulatory body shall be met.
b) Wagering using funds from player accounts and/or electronic payment accounts shall meet the applicable "Cashless Device Requirements" of the *GLI-16 Standards for Cashless Systems and Technologies* and/or other applicable technical requirements observed by the regulatory body.

Chapter 6: Wagering Requirements

6.1 Introduction

6.1.1 General Statement

This chapter sets forth the technical requirements for information required to be made available regarding the wagering events, markets, and wager types available on the Event Wagering System, and the methods for placing a wager on the Wagering Platform.

6.2 Player Interface Requirements

6.2.1 Player Interfaces

The player interface is an interface application or program through which the player views and/or interacts with the Remote Player Device or Self-Service Wagering Terminal, including the touch screen, keyboard, mouse, button panel, or other forms of player interaction devices. The player interface shall meet the following requirements:

a) Any orientation change, resizing, or overlay of the player interface screen shall be mapped accurately to reflect the revised display and touch/click points or buttons.
b) All player-selectable touch/click points or buttons represented on the player interface screen that impact wagering activities shall be clearly labeled according to their function and shall operate as disclosed to the player.
c) There shall be no hidden or undocumented touch/click points or buttons anywhere on the player interface screen that impact wagering activities.
d) Wagering instructions, as well as information on the functions provided by the player interface, shall be clearly communicated to the player and not be misleading or inaccurate.

6.2.2 Adaptive Displays

The display of the wagering instructions and information shall be adapted to the player interface. For example, where a device or terminal 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.

6.2.3 Alternating Displays

Where multiple items of wagering instructions and information are displayed on the player interface, it is acceptable to have these items displayed in an alternating fashion provided that the rate at which the instructions and information alternates permit the player a reasonable opportunity to read each item.

6.2.4 Simultaneous Inputs and Outputs

Simultaneous or sequential activation of various inputs and outputs, including player interaction devices comprising a player interface, shall not, whether intentionally or not, cause wager malfunctions or invalid results.

6.3 Wagering Displays and Information

6.3.1 Posting of Wagering Rules

Comprehensive wagering rules shall be posted for the wagering events, markets, and wager types currently offered (moneyline, point spreads, over/under, win/place/show, parlay, etc.). Where the player interface includes these wagering rules directly, the software shall be evaluated against the requirements within the "Wagering Rules" section of this document.

6.3.2 Dynamic Wagering Information

The following information shall be made available to the player without the need for placing a wager. Within a Wagering Venue this information may be displayed by a Retail Wagering Terminal directly and/or by an external display:

a) Information regarding the available wagering events, markets, and wager types;
b) Current odds/payouts and prices for the available wagering events, markets, and wager types;
c) For pari-mutuel wagering:
   i. Up-to-date odds and/or estimated payouts for market pools. It is acceptable that, for complex pools, such estimates may be subject to reasonable limitations in accuracy;
   ii. Up-to-date total amounts wagered (pool totals) for each market pool; and
   iii. Declared dividends for settled markets.

NOTE: This information shall be displayed as accurately as possible within the constraints of communication delays and latencies.

6.3.3 Rakes, Commissions, and Fees

There shall be sufficient information available to the player regarding charges imposed on players or award payout adjustments such as a rake, commission, or fee taken by the operator, as applicable. Any variation in the published information shall be disclosed to the player.

6.3.4 Event Wagering Jackpots

Where allowed by the regulatory body, outcomes of wagering events and markets may result in winning additional monetary awards or "jackpot payoffs" which increase based on wagering as follows:

a) Progressive jackpots increase according to the amounts wagered on the wagering event or market.
b) Incrementing bonus jackpots behave identically as progressive jackpots, except they increase

based on the occurrence of one or more specific conditions established by the wagering rules instead of, or in addition to, increases based on amounts wagered.

NOTE: The offering of progressive jackpots and incrementing bonus jackpots within event wagering, shall meet the applicable requirements of the *GLI-19 Standards for Interactive Gaming Systems* (for remote wagering) and/or the *GLI-12 Standards for Progressive Jackpots* (for retail wagering).

6.4 Wager Placement

6.4.1 Placement of a Wager

The Wagering Platform shall clearly inform the player of all wagering events, markets, and wager types available for wagering on before the player commits to placing a wager. The following requirements apply to the selection and placement of a wager on the player interface:

a) The method of placing a wager shall be straightforward, with all wager selections (including their order, if relevant) identified. When the wager involves multiple wagering events or markets (e.g., parlays), such groupings shall be identified.
b) Players shall have the ability to select the wagering event, market, and wager selection they want to place a wager on.
c) Wagers shall not be automatically placed on behalf of the player without the player's consent/authorization.
d) Players shall have an opportunity to review and confirm their selections before the wager is submitted. This does not preclude the use of "single-click" wagering where permitted by the regulatory body and opted in by the player.
e) The Wagering Platform shall prevent multiple wagers from being placed that arise from communications errors or pressing the wager purchase touch/click point or button repeatedly while awaiting a response from the platform.
f) Clear indication shall be provided that a wager has been accepted or rejected, including the amount of the wager and the odds/payouts accepted by the system. When multiple wagers are placed at once, each wager shall be acknowledged and clearly indicated separately so that there is no doubt as to which wagers have been accepted.
g) Amounts wagered shall be subtracted from the funds available for wagering when the wager is accepted by the system. A wager shall not be accepted that could cause the player to have a negative balance.
h) Where allowed by the regulatory body, the platform may allow a player to specify an odds/payout or price condition, and/or any other conditions, related to a wagering event or market at which a qualifying wager will be automatically placed when such conditions are met or exceeded. Where this functionality is supported:
    i. The functionality and available condition-based wager options shall be clearly explained to the player;
    ii. The player shall be able to create and remove condition-based wager requests.
    iii. Player accounts shall reflect any funds held for condition-based wagers.
    iv. All pending condition-based wager requests shall be displayed to the player.
    v. Where a player manually places a wager, any pending condition-based wager requests associated with that wager shall be cancelled.

6.4.2 Free Bet/Demo Mode

Free bet/demo mode allows a player to simulate wagering without paying, principally for the purpose of learning or understanding wagering mechanics. If the Wagering Platform supports a free bet/demo mode, the following requirements apply:

a) Free bet/demo mode shall accurately represent the normal operation of paid wagering. Free bet/demo mode shall not mislead the player about the odds/payouts available in the paid version;
b) Free bet/demo mode shall be prominently displayed so a player knows at all times if/when this mode is active; and
c) Free bet/demo mode shall not update the player's funds available for wagering. Specific accounting is permissible for this mode provided the meters clearly indicate as such.

NOTE: Paid wagers using credits received from a bonusing/promotional offer are not considered a part of free bet/demo mode.

6.4.3 Player Resource Feature

Unless prohibited by the regulatory body, a player resource feature may be offered that provides advice, hints, or suggestions to a player. An illustrative example might be a data stream that may be used to externally facilitate wager selection.

a) The player resource feature shall clearly describe to the player that it is available and any advantage it offers;
b) The method for obtaining the player resource feature and what options exist for selection shall be disclosed to the player.
c) Any player resource feature that is offered to the player for purchase shall clearly disclose the cost and benefit;
d) The player resource feature shall not be misleading or inaccurate, and shall reflect the rules in relation to this feature, while noting that the rules may change as a function of the resource offered, providing that any such changes are disclosed to the player prior to acceptance of the resource;
e) The player resource feature shall allow the player the option of accepting any assistance, and shall not force the player to accept the assistance unless it reflects the only possible option for the player to pursue at the time; and
f) The availability and content of the player resource feature shall remain consistent unless otherwise disclosed and shall not adapt in a way that disadvantages the player based upon prior wagers.

6.4.4 Changes During Fixed Odds Wager Placement

For fixed odds wagers, the Wagering Platform shall identify situations where the attributes of the associated wager selection (e.g., odds/payouts, prices, etc.) have changed prior to acceptance of the wager.

a) If the revised wager selection is more favorable to the player, the wager may be accepted automatically, provided the player is notified of the updated values, and such functionality is clearly explained to the player.
b) If the revised wager selection is less favorable to the player, the wager shall not be accepted unless the player explicitly confirms acceptance of the updated values, unless the player has previously opted in to an auto-accept function for less favorable changes. Where this functionality is supported:
    i. The functionality and available auto-accept options shall be clearly explained to the player;
    ii. The player shall manually opt in to use this functionality (i.e., it shall not be enabled by default); and
    iii. The player shall be able to opt out at any time.

6.4.5 Layoff Wagers

Where permitted by the regulatory body, a Wagering Platform may support layoff wagers received from external operators. Where layoff wagers are supported:

a) Each layoff wager shall be manually entered into the platform only by authorized personnel.
b) The platform shall provide a secure means for entering layoff wagers received from external operators and shall log each wager entry with a reference to the authorized personnel who performed the entry.
c) Each external operator placing layoff wagers shall be uniquely identified within the Wagering Platform, and each layoff wager shall be associated with the external operator from which the wager was received.

NOTE: For layoff wagers placed with external operators by authorized personnel, the Wagering Platform may be used to record the external layoff wager and adjust the risk analysis values stored and reported by the system.

6.4.6 Wager Record

Upon completion of a wager transaction, the player shall have access to a wager record which contains the following information, as applicable:

a) The date and time the wager was placed;
b) Each player choice involved in the wager:
    i. The description of the wagering event, market, and wager type (e.g., moneyline, point spreads, over/under, win/place/show, parlay, etc.);
    ii. Wager selection (e.g., athlete or team name and number) or combination of selections chosen, including selection names where practical;
    iii. The date and time the wagering event will be expected to occur or has occurred, if known;
c) Odds/payouts applicable at the time the wager was placed;
d) Total amount wagered, separately indicating any bonusing/promotional amounts;
e) Any special conditions applying to the wager;
f) Unique wager record ID and/or barcode of the wager;
g) For retail wagers, the unique user account ID, unique terminal ID, or equivalent which issued the wager record;

h) For a printed wager record, it is permissible for the following information to be contained on the ticket stock itself:
   i. Wagering Venue Name/Site ID; and
   ii. Redemption period.

NOTE: Some of the above-listed information may also be part of the unique wager record ID and/or barcode. Multiple barcodes are allowed and may represent more than just the unique wager record ID.

6.4.7 Wagering Period Close

It shall not be possible to place wagers on a wagering event or market once the wagering period for that wagering event or market has closed.

6.5 Results and Payment

6.5.1 Results Display

Results entry shall include the entry of all information which may affect the results of all markets offered for that wagering event.

a) It shall be possible for a player to obtain the results of their wagers on any settled market once the results have been confirmed.
b) Wagers shall be settled in accordance with the wagering rules applicable to that wagering event, market, and wager type.
c) The Wagering Platform shall facilitate the ability to retrieve market results on any completed market for a period of time as described in the wagering rules.
d) The Wagering Platform shall be able to modify a market result when circumstance permits until the result has been confirmed, and the operator shall obtain regulatory body approval of any such method.
e) Following circumstances when a market result has been modified (e.g., due to statistics/line corrections), the changes of results shall be made available.
f) For pari-mutuel wagering, the dividends on any completed market shall be made available, including any new dividends calculated based on any changed results.

6.5.2 Early Settlement Feature

The Wagering Platform may offer a feature for the player to perform an early settlement of their wager for an adjusted payout before the wagering event's conclusion. The early settlement feature shall only be supported for wagers comprised entirely of wager selections designated as eligible for early settlement. Availability of early settlement may be modified or withdrawn at any time.

a) The early settlement feature shall clearly describe to the player that it is available, and any rules or conditions relevant to the early settlement feature, to enable the player to make an informed decision as to whether to request early settlement.
b) Wagers that are eligible for early settlement shall be clearly indicated along with an adjusted payout amount. The adjusted payout amount will depend on the current state of the wagering event and the time elapsed and may be higher or lower than the original amount of the wager.

c) The Wagering Platform may allow a player to specify an adjusted payout threshold or other specified conditions related to a wagering event or market at which early settlement for a qualifying wager will be automatically processed when such threshold or conditions are met or exceeded.
   i. The player shall be able to create and remove condition-based settle requests.
   ii. All pending condition-based settle requests shall be displayed to the player.
   iii. Where a player manually executes an early settlement, any pending condition-based settle requests associated with that wager shall be cancelled.
d) If the early settlement is processed, a confirmation message shall be displayed, and the wager shall be settled for the adjusted payout amount. Subsequent wagering event outcome shall not affect the settled wager or its payout amount.
e) If the early settlement feature is not available, or a condition-based settle request is not triggered prior to the confirmation of the market's result, the wager shall be settled normally based on the final market outcome.
f) Where an early settlement is issued in error, there shall be a mechanism to void the early settlement and settle the original wager normally based on the final market outcome using the correct odds/payouts.

6.5.3 Wager Redemption

Once the outcomes of the market are entered and confirmed, or once early settlement has been processed, the player may redeem and receive payment for their wagers.

a) For account-based wagers, the wager record shall be automatically redeemed and the amounts paid shall be added to the player account balance, except for merchandise and large wins or payouts where required by the regulatory body.
b) For anonymous wagers, the wager record can be redeemed by any Retail Wagering Device which supports wager record redemption provided that no amounts shall be paid to the player prior to confirmation of wager record validity.

6.6 Peer-to-Peer (P2P) Wagering

6.6.1 P2P Wagering

Peer-to-Peer (P2P) wagering involves environments which offer players the opportunity to wager with and against each other. In these environments, the operator usually does not engage in the wagering as a party but usually provides the environment for use by its players, and may take a rake, commission, or fee for the service. The following requirements apply:

a) Players shall be prevented from competing against themselves unless authorized by the applicable wagering rules;
b) If player resource features are offered which may provide a player with an advantage over other players, players shall be provided with sufficient information to make an informed decision, prior to participation in, as to whether to compete against players who may possess such features;
c) Players shall be provided with appropriate warnings where the use of bots, scripts, or other unauthorized software can affect wagering so that they can make an informed decision whether to participate; and

d) It shall be explicitly indicated to the player on the wagering screen while sponsored players are competing against them.

6.6.2 Pot/Pool Display

Where players are competing for a specific pot or pool, the pot or pool amount for which they are competing shall be clearly displayed to each player and shall be updated each time a wager is placed or whenever the pot or pool amount otherwise changes in accordance with the applicable wagering rules.

6.6.3 Reporting Suspicious Players

Players shall be provided with a mechanism to report suspected cheating, collusion, or usage of bots, scripts, or other similar software by others to create an unfair advantage.

6.7 Exchange Wagering

6.7.1 General Statement

Exchange wagering involves two or more players place identically opposing wagers, allowing players to wager on both winning and non-winning outcomes in the same wagering event or market.

6.7.2 Market Maker Wagers

The Wagering Platform shall clearly disclose the presence of wagers for sale or for purchase by, or posted on behalf of, a market maker.

6.7.3 Wager Formalization

A wager to back or lay a particular wager selection in a given market, specifying the odds/payouts and prices of the wager, shall be placed directly with the operator by the player. The Wagering Platform shall:

a) Only formalize a wager upon the successful matching of the pending wager;
b) Allow pending wagers to be modified or cancelled prior to matching;
c) Automatically cancel unmatched pending wagers upon expiry or wagering period closure; and
d) Ensure that once a pending wager is matched to identically opposing wagers, it is final and shall not be cancelled except as permitted by the wagering rules or the regulatory body.

6.7.4 Best Execution

The Wagering Platform shall match pending wagers using a “best execution” methodology, ensuring wagers are matched at the most favorable odds/payouts available that are equal to or better than those requested by the player. The Wagering Platform shall:

a) Support full or partial matching of pending wagers to identically opposing wagers;

b) Continue matching any unmatched portion at the most favorable odds/payouts until fully matched or no qualifying opposing wagers remain;
c) Prioritize matching based on odds/payouts and time of submission;
d) Treat any modification to a pending wager, including changes to wager amount, as a new wager for matching priority;
e) Not apply any undisclosed margin between matched wagers; and
f) Provide players the option to display available exchange wagering liquidity at the most favorable odds/payouts, including the opposing wagers available for matching.

6.7.5 Live Exchange Wagering Delays

For exchange wagering involving live-event wagers, the Wagering Platform shall apply a delay before pending wagers are accepted and matched.

a) The delay shall ensure fair and equitable treatment of players across different access channels.
b) Wagers submitted during the delay period shall not be accepted or matched until the delay has elapsed.
c) The delay shall not apply to the cancellation of unmatched pending wagers.

6.8 Virtual Event Wagering

6.8.1 General Statement

Virtual event wagering allows for the placement of wagers on computer-generated simulations of, or previously recorded, wagering events in which virtual participants compete with one another as allowed by the regulatory body. The applicable requirements detailed within this section shall apply to virtual event wagering along with the other applicable requirements of this chapter. Nothing in this section should be interpreted as being applicable to wagering on live, real-world wagering events.

6.8.2 Virtual Wagering Event Randomization

A virtual wagering event may utilize the random properties of a cryptographic RNG to impact the event's outcome, contributing event elements, or sequence of event elements, in which case, the requirements as found within the "Random Number Generator (RNG) Requirements" chapter and "Game Outcome Using a Random Number Generator" section of the *GLI-19 Standards for Interactive Gaming Systems* (for remote wagering) and/or the *GLI-11 Standards for Gaming Devices* (for retail wagering). shall be met as applicable.

NOTE: Implementations of virtual event wagering which do not rely on the use of an RNG will be evaluated on a case-by-case basis by the independent test laboratory.

6.8.3 Virtual Wagering Event Display and Fairness

Virtual wagering events shall conform to applicable requirements regarding "Game Information and Rules of Play", "Information to be Displayed", and "Game Fairness" within the *GLI-19 Standards for*

Interactive Gaming Systems (for remote wagering) and/or the *GLI-11 Standards for Gaming Devices* (for retail wagering). In addition, the following requirements apply:

a) Statistical data that is made available to the player pertaining to the virtual wagering event shall not misrepresent the capabilities of any virtual participant. Depending on the type of virtual wagering event, this does not prevent the use of an element of chance or randomness from impacting performance of the virtual participant during the virtual wagering event as provided for by design.
b) It shall not be possible to ascertain the outcome of the virtual wagering event prior to its commencement.
c) For scheduled virtual wagering events, a countdown of the time remaining to place a wager in that event shall be displayed to the player. It shall not be possible to place wagers on the event once this time has passed; however, this requirement does not prohibit the implementation of live-event wagers depending on the type of virtual wagering event.
d) After the commencement of a virtual wagering event, no further actions or decisions may be made that change the behavior of any of the elements of chance within the virtual wagering event, other than player decisions.
e) Each virtual participant shall be unique in appearance, where applicable to the wager. For instance, if the wager is on one team to beat another, the virtual participants themselves do not need to be unique in appearance, however the teams that they are on shall be visually distinct from each other.
f) The outcome of a virtual wagering event shall be clear, unambiguous, and displayed for a sufficient length of time to allow a player a reasonable opportunity to verify the result of the wagers related to that virtual wagering event.

6.8.4 Virtual Wagering Event Recall

All information necessary to adequately reconstruct the virtual wagering events, including the virtual wagering event outcome and/or virtual participant actions, shall be recorded by the Wagering Platform or associated equipment, using some combination of text, logs, video, graphics, screen captures, or other means (e.g., "flight recorder" mechanism).

6.9 External Wagering Platforms

6.9.1 General Statement

This section contains requirements for the circumstances where the Wagering Platform communicates with an external wagering platform in any of the following configurations:

a) The Wagering Platform is acting as the "host wagering platform" receiving, for its own wagering events and markets, wagers from one or more external "guest wagering platforms"; or
b) The Wagering Platform is acting as a "guest wagering platform" passing wagers to one or more external "host wagering platform," for those platforms' wagering events and markets.

NOTE: The requirements of this section apply to the interoperability of the Wagering Platform with the external wagering platform and is not a complete evaluation of the external wagering platform itself. The external

wagering platform may independently be subject to evaluation by the independent test laboratory per regulatory body discretion.

6.9.2 Communications with External Wagering Platforms

The following requirements apply to information being conveyed between the host wagering platform and the guest wagering platform:

a) Authentication shall occur between the host wagering platform and the guest wagering platform prior to transactions being conducted.
b) The correct delivery of wager transactions shall not be affected by characteristics of the communication channel such as bandwidth, delay, bit error rate and link utilization.
c) The host wagering platform shall correctly process all wager transactions. Incomplete transactions shall be reversed under the following circumstances:
    i. Communication is lost between the host wagering platform and the guest wagering platform.
    ii. Extended communication delays occur between the host wagering platform and the guest wagering platform. Manual reversal of transactions is permitted provided that the reports in-determinate transactions to the operator.
d) If the host wagering platform provides fixed odds wagering for the guest wagering platform where the odds/payouts and prices can be dynamically changed, the Wagering Platform shall be able to:
    i. When acting as the guest wagering platform, receive the current odds/payouts and prices sent from the host wagering platform whenever any odds/payouts and prices are changed.
    ii. When acting as the host wagering platform, pass the current odds/payouts and prices to all receiving guest wagering platforms whenever any odds/payouts and prices are changed.
e) If the host wagering platform provides pari-mutuel wagering for the guest wagering platform, the Wagering Platform shall be able to:
    i. When acting as the guest wagering platform, receive the current dividends for active pools sent from the host wagering platform.
    ii. When acting as the host wagering platform, pass the current dividends for active pools to all receiving guest wagering platforms.
f) Change of wagering event status information shall be passed from the host wagering platform to the guest wagering platform whenever any change occurs, including:
    i. Withdrawn/reinstated wager selections;
    ii. Altered wagering event starting time;
    iii. Wagering period for markets opened/closed;
    iv. Results entered/modified;
    v. Results settled; and
    vi. Wagering event or market cancelled.

6.9.3 External Wager Placement

The following requirements apply to wagers being placed between the host wagering platform and the guest wagering platform:

a) Wagers passed from the guest wagering platform to the host wagering platform shall include the amount to be wagered and the expected odds/payouts, as advertised at the time of placement of the wager on the host wagering platform.
b) The host wagering platform shall accept or reject wagers received from a guest wagering platform on the basis of the current status of the wagering event or market at the time the wager is received rather than at the time of the wager being placed by the guest wagering platform.
c) If the wager is accepted from a guest wagering platform, it shall be at the odds/payouts currently established on the host wagering platform not as expected by the guest wagering platform.
d) The host wagering platform shall send clear acknowledgment of any wager from the guest wagering platform, including indication of partial acceptance and the odds/payouts established by the host wagering platform.
e) Wagers placed on the guest wagering platform shall receive clear acknowledgment of acceptance, partial acceptance, or rejection sent by the host wagering platform.
f) The wager acknowledgment from the host wagering platform shall include the following details as applicable:
    i. The odds/payouts given by the host wagering platform, especially if different from the expected odds/payouts.
    ii. Indication of partial wager acceptance, including the amount partially accepted.
    iii. The total wager cost.
g) If the cost of the wager is determined by the host wagering platform, there shall be a positive confirmation sequence in place to enable the player to accept the wager cost and the guest wagering platform 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 platform.
h) Where wagers may be placed in bulk, the following requirements apply:
    i. If the stream of wagers is interrupted for any reason, there shall be a means available to determine where in the stream that the interruption occurred.
    ii. No wager in the stream may be greater than the account balance. If such a wager is attempted, the entire stream is to be halted.
i) The account balance shall be debited an amount equaling the offer and cost to the host wagering platform. The funds shall remain as a pending transaction with details of the offer to the host wagering platform logged. On receipt of acknowledgment from the host wagering platform, the appropriate adjustments shall be made to the "pending" account and the account balance on the guest wagering platform.

6.9.4 External Wager Cancellations

Cancellation requests from the guest wagering platform shall receive clear acknowledgment of acceptance or rejection by the host wagering platform.

a) If the cancellation is rejected, the reason for the rejection shall be forwarded from the host wagering platform to the guest wagering platform and then to the player.
b) The player is not to be credited by the guest wagering platform until final confirmation is received from the host wagering platform including the amount of the cancelled wager.

6.9.5 External Wager Settlement

When results are entered and confirmed on the host wagering platform, or received from another host wagering platform, each settled wager placed from a guest wagering platform shall be transferred by the host wagering platform to the guest wagering platform with the paid amount, as applicable.

a) Confirmation of receipt of the settled wagers shall be acknowledged by the guest wagering platform.
b) Player accounts on the guest wagering platform are to be handled by the guest wagering platform including updating of the amounts paid in those accounts where applicable.

6.10 Spectator Wagering Requirements

6.10.1 General Statement

Where authorized by a regulatory body, the following requirements apply where a spectator player's wagering activities are tied to the wagers of a host player. Details on the host player's wagers are accessible to all spectator players. The wagers placed by the host player shall meet the requirements of this standard.

6.10.2 Wager and Player Display

The player interface shall clearly indicate to the spectator player where wagers, player choices, and/or results are based on the host player's wagering.

a) Information shall be available to fully describe the spectator wagering functionality, including a clear explanation of all settings and default options for both host players and spectator players.
b) A host player shall be able to control whether or not they want to allow for spectator players.
c) Spectator players shall have the same access to the wagering rules, and the same odds/payouts and prices for the wager being placed by the host player as they would if the spectator players were placing the wager themselves.
d) The host player's wagers and results shall not be modified or influenced by the presence of spectator players, or by spectator player activity, volume of wagers, or wager results.
e) The Wagering Platform shall not provide the host player with information on the spectator players' wagers, which may influence the choices made by a host player.
f) A host player shall be clearly indicated to the spectator players if they are a sponsored player.

6.10.3 Linked Wagering

Linked wagering occurs when a spectator player's wager is tied directly to each wager of a host player, such that identical wager results (wins and losses) are applied proportionally to the spectator player's account.

a) Proportionality rules (e.g., bet scaling, payout ratios) shall be disclosed to the spectator player prior to wager placement.
b) The spectator player's linked wagers shall be settled simultaneously with the host player's wager settlement.

c) The spectator player may opt in or out of subsequent linked wagers but may not retroactively cancel or alter wagers after the host player's wagers have been placed.

6.10.4 Performance-Based Wagering

Performance-based wagering occurs when a spectator player places a wager on measurable outcomes derived from one or more host player's completed games (e.g., "win/lose", "total amount won on fifty wagers", "number of wagers won in three days", etc.).

a) Each performance wager shall clearly specify the metric being wagered on, the settlement condition, and the odds/payout or price structure.
b) Performance wagers may only be placed before any contributing host player's wagers have settled.
c) The host player shall not be able to see which spectator player's wagers are placed on their performance.

Appendix A: Internal Control Procedures and Practices

A.1 Introduction

A.1.1 General Statement

This appendix sets forth internal control procedures and practices for event wagering operations which will be reviewed in an internal controls audit, including, but not limited to establishing wagering rules, suspending events, handling various wager and financial transactions, creating markets, settling wagers, closing markets, cancellations of events, voiding or cancelling wagers, player account management, fundamental practices relevant to the limitation of risks, and any other objectives established by the regulatory body.

NOTE: It is also recognized that additional procedures and practices which are not specifically included within this standard will be relevant and required for an operational audit as determined by the operator and/or regulatory body within their rules, regulations, and Minimum Internal Control Standards (MICS).

A.2 Internal Control Procedures

A.2.1 Internal Control Procedures

The operator shall establish, maintain, implement and comply with internal control procedures for event wagering operations, including performing wager and financial transactions.

A.2.2 Information Management

The operator's internal control procedures shall include the processes for maintaining the recorded information specified under the section entitled "Information to be Maintained", and other logs or records required by this standard unless specified otherwise, for a period of five years or as otherwise specified by the regulatory body.

A.2.3 Risk Management

The operator's internal control procedures shall contain details on its risk management framework, including but not limited to:

a) Automated and manual risk management procedures;
b) Employee management, including access controls and segregation of duties;
c) Information regarding identifying and reporting fraud and suspicious conduct;
d) Controls ensuring regulatory compliance;
e) Description of Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF) 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 forms of event wagering available to be offered by the operator;
h) Description of all integrated third-party service providers; and
i) Any other information required by the regulatory body.

A.2.4 Use of Third-Party Service Providers

The operator's internal control procedures shall identify any third-party service provider involved in supporting or performing functions subject to the operator's internal control procedures. This shall include, at a minimum, the identity of the third-party service provider, a description of the services provided to the operator (e.g. geolocation, know-your-customer, payment processing, statistics/line data, etc.), the provider's roles and responsibilities, and the operator's procedures for evaluating the adequacy of, and monitoring compliance with, the provider's applicable controls, procedures, and contractual or regulatory obligations.

a) The operator shall maintain processes to ensure that:
   i. The collection, use, and disclosure of sensitive information by or through the third-party service provider is limited to the information necessary to provide the applicable service.
   ii. The third-party service provider's protection of sensitive information is evaluated and verified, as applicable to the nature of the service provided; and
   iii. Communications between the operator and the third-party service provider conveying sensitive information are encrypted and protected against unauthorized access, interception, or alteration.
b) When an incident or error occurs that results in a loss of communication with, or other failure of, the third-party service provider's services that affect the operational system, the incident or error shall be recorded in a log containing the date and time of occurrence, its duration, nature, a description of its impact on the system's performance, and it's resolution if resolved.

A.2.5 Prohibited or Restricted Persons

There shall be a method described in the operator's internal controls to identify and implement the following regarding prohibited or restricted persons:

a) Employees, subcontractors, directors, owners, and officers of an operator, as well as those within the same household shall not place wagers on any wagering event, unless using clearly marked test accounts for testing purposes;
b) Individuals identified to be any of the following shall not place wagers on any wagering events:
   i. Underage, or using the PII of a deceased person;
   ii. On any suspension lists held by the operator;
   iii. On any exclusion lists that may be provided by the regulatory body;
   iv. Placing wagers on behalf of another person, unless authorized by the regulatory body; or
   v. Prohibited from event wagering for any other reason.
c) 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 sporting event or game, competition, contest, match, race, or other occurrence or type of activity in which they participate, the athlete they represent participates, or they may have insider information.

A.2.6 Workstation Access Controls

The operator's internal control procedures shall include controls for securing workstations used to perform regulated functions of the Event Wagering System, including procedures to ensure that:

a) Access to workstations by an individual is controlled by a secure logon procedure or other secure process approved by the regulatory body to guarantee that only authorized personnel are allowed access.
b) It is not possible to modify the configuration settings of the system without an authorized secure process.
c) If user sessions are supported by the workstation:
    i. A user session is initiated by the individual logging in to their user account using their secure username and password or an alternative means for the individual to provide authentication credentials as allowed by the regulatory body.
    ii. All available options presented to the individual are tied to their user account.
    iii. If the workstation does not receive input from the individual within fifteen minutes, or a period specified by the regulatory body, the user session times out or locks up, requiring the individual to re-establish their login in order to continue. For mobile workstations, the period shall not exceed two minutes unless otherwise specified by the regulatory body.
    iv. User accounts are automatically locked-out after three consecutive failed access attempts in a thirty-minute period, or a period to be determined by the regulatory body. Where supported, a mechanism may be used which automatically releases a locked-out account after thirty minutes, or a period to be determined by the regulatory body, has elapsed.

NOTE: It is acceptable for this section to be met by an off-the-shelf operating system which is installed on the same server.

A.2.7 Test Accounts

The operator may establish test accounts to be used to test the various components and operation of an Event Wagering System in accordance with internal control procedures adopted by the operator, which, at a minimum, shall address procedures for:

a) Authorizing testing activity and assigning each test account for use;
b) The issuance and segregation of funds used for testing, including the identification of who is authorized to issue the funds, the maximum amount of funds that may be issued, and the purpose for which the issued funds may be used;
c) Maintaining a record for all test accounts, to include when they are active and to whom they are issued; and
d) Auditing testing activity to ensure the accountability of funds used for testing and proper adjustments to reports and records.

A.3 General Operating Procedures

A.3.1 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 used to cover all other operator liability where required by the regulatory

body.

A.3.2 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 segregated account or 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.3.3 Taxation

Where the regulatory body has taxation procedures, the operator shall have a process in place to identify all payouts that are subject to taxation (single payouts or aggregate payouts over a specific time period as required).

NOTE: Payout amounts exceeding any jurisdiction-specified limit shall require the appropriate documentation to be completed before the player is paid.

A.3.4 Complaint/Dispute Process

The operator shall provide a method for a player to make a complaint/dispute, and to enable the player to notify the regulatory body if such complaint/dispute has not been or cannot be addressed by the operator, or under other circumstances as specified by the law of the regulatory body.

a) Players shall be able to log complaints/disputes on a 24/7 basis.
b) Records of all correspondence relating to a complaint/dispute shall be maintained by the operator.
c) A documented process shall exist between the operator and the regulatory body on the complaint/dispute reporting and resolution process, with response times and escalation to an independent external channel where the regulatory body provides one.

A.3.5 Chat Features

Procedures shall exist for cases where the operator provides for the use of chat features which allow the player to communicate directly with the operator and/or other players.

a) The operator shall maintain chat logs and email correspondence between the player and the operator for a period of ninety days or as required by the regulatory body;
b) When a player interacts with a chatbot or virtual assistant:

i. The player shall be clearly notified that they are interacting with a chatbot or virtual assistant, not a human;
ii. The player shall be provided with contact information or functionality to request to interact with a human representative; and
iii. The operator shall implement a process for the periodic human review of interaction logs between the player and the chatbot or virtual assistant, which assesses the chatbot's or virtual assistant's performance for accuracy, sentiment, and adherence to the operator's internal control procedures.

A.3.6 Responsible Gaming Plan

The operator shall have a responsible gaming plan, containing policies and procedures to promote responsible gaming. The operator shall maintain evidence that the relevant policies and procedures were followed and present such evidence to the regulatory body upon request. The responsible gaming plan shall include:

a) Measures and processes to detect and identify problem gambling, and actions and/or behavior which is indicative that a player is at risk of developing a gambling problem. These measures and processes may include, but are not limited to, using analytical tools and/or behavior monitoring mechanisms with pre-designed and/or evolving parameters, and player facing and/or responsible gaming personnel.
b) Policies and procedures governing the actions that shall be taken by the operator with respect to problem gamblers and players who are at risk of developing a gambling problem.
c) Recordkeeping of any internal responsible gaming investigation carried out on a player, any decisions taken on the basis of the operator's responsible gaming policies and procedures, and player interactions, which shall consist of a clear and detailed audit trail that shall be made available to the regulatory body upon request.
d) Responsible gaming training upon hire and regularly thereafter for personnel who are responsible for dealing with responsible gaming-related matters, and for player interaction in general.
    i. The operator shall keep a record of the personnel required to complete the training, the type and frequency of training, and the responsible gaming training and testing undertaken.
    ii. The personnel shall be trained to understand problem gambling issues, know how to respond to them, and look out for players demonstrating signs or indications of gambling-related harm.
e) Applicable standards of socially responsible advertising, including compliance with all observed rules and regulations, and encouraging affiliates, which may include content providers, social media influencers, social media accounts, and brand ambassadors, to also adhere to these standards.
f) Procedures for evaluating and continuously monitoring the responsible gaming plan and initiatives.

NOTE: The regulatory body may require a responsible gaming plan to undergo an independent third-party evaluation against industry standards for responsible gaming or other requirements as required by the regulatory body.

A.3.7 Personally Identifiable Information (PII) Security

Any information obtained with respect to a player, including personally identifiable information (PII) and funds-related information, shall be handled in compliance with the operator's privacy policy, and applicable privacy laws, regulations, and standards observed by the regulatory body. PII and funds-related information shall be treated as critical assets for risk assessment purposes.

a) PII and funds-related information shall be kept confidential and disclosed only where authorized by the privacy policy or regulatory requirements. This includes, but is not limited to:
   i. The amount of funds credited to, debited from, or present in any particular player account;
   ii. The amount of funds wagered by a particular player on any wagering event or market;
   iii. The player account ID and authentication credentials that identify the player; and
   iv. The name, address, and other information in the possession of the operator that would identify the player to anyone other than the regulatory body or the operator.
b) There shall be procedures in place for the security and authorized sharing of PII and funds-related information as required by the regulatory body, including, but not limited to:
   i. The designation of one or more employees having primary responsibility for the design, implementation, and ongoing evaluation of such procedures and practices;
   ii. The nature and scope of all information collected, the locations in which it is stored, and the servers or storage devices which may be used for storage or transfer;
   iii. Measures to protect information from unauthorized access; and
   iv. Procedures for responding to a data security breach, including notification to the regulatory body where required.
c) Where required by the regulatory body, players shall be provided with a method to request:
   i. Access and updates to their PII;
   ii. Confirmation that their PII is being processed and information about the PII processing;
   iii. The forwarding of PII received from the player, in a structured, commonly used, and machine-readable format, and transmission of those data to another operator, where technically feasible, provided that such PII was provided by the player or is processed by automated means, and the basis for processing is PII consent or fulfilment of a contract or preparatory steps to a contract; and
   iv. Objection to PII processing based on legitimate interests, the performance of a task in the public interest or in the exercise of official authority, direct marketing, including related profiling, or scientific or historical research purposes or for the purpose of statistics; and
   v. Erasure of their PII or restriction of PII processing where the PII is no longer necessary for the purpose for which it was collected or processed, the player withdraws consent, the player objects to the processing and there is no overriding legitimate basis to continue, the PII was unlawfully processed, or erasure is required to comply with a legal obligation.
d) There shall be procedures in place to record, process, and respond to the requests from players described in this section, including, but not limited to:
   i. Maintaining records of such requests;
   ii. Complying with such requests as required by the regulatory body; and
   iii. Providing the player with any denial or rejection reasons and information on the possibility to file a complaint/dispute with the regulatory body.
e) Where prohibited by the regulatory body, the operator may not utilize solely automated decision-making which:

i. Produces legal effects the player such as those which result in the player being subjected to surveillance by a competent authority; or
ii. Significantly affects the player in a similar manner (e.g., it has the potential to influence the circumstances, behavior or choices of the player).

A.3.8 Payment Processing Security

The operator or a third-party financial service provider used to conduct transactions with financial institutions shall protect payment methods used in the system from fraudulent use. There shall be established procedures:

a) To reconcile all financial transactions between the operator and the financial service provider daily or as otherwise specified by the regulatory body;
b) To protect any payment method used from fraudulent use; and
c) For assuring the ownership of the payment method with the identity of the player to avoid fraud and money laundering.

NOTE: The regulatory body may require a financial service provider used to process transactions to undergo an independent third-party evaluation against industry standards for payment security, such as the Payment Card Industry Data Security Standards (PCI-DSS), or other requirements as required by the regulatory body.

A.4 Operator Display Content

A.4.1 Operator Display Content

Operator display content refers to any written, graphical, and auditory information provided to the public regarding event wagering operations.

a) Operator display content shall be complete, unambiguous, and not misleading or unfair to the player.
b) Operator display content that is presented aurally (via sound or voice) shall also be displayed in written form.
c) Operator display content shall be rendered with sufficient font size and clarity in a color that contrasts with the background color to ensure that all information is clearly visible/readable.
d) Operator display content shall contain the same information and carry the same meaning across all languages it is provided in.
e) The operator shall keep a log of any changes to the operator display content.

NOTE: Within a Wagering Venue this content may be displayed by a Retail Wagering Terminal directly and/or by external signage, forms, or brochures available.

A.4.2 Wagering Rules

The operator shall adopt and adhere to comprehensive wagering rules which shall be approved by the regulatory body and made available to the player. Where wagering rules are altered for wagering events, markets, and wager types being offered, all rule changes shall be time and date stamped

showing the rule applicable in each period. If multiple rules apply to a wagering event, market, and wager type, the operator shall apply the rules that were in place when the wager was accepted:

a) The methods of funding a wager or player account (e.g., cash, personal check, cashier's check, wire transfer, money order, credit or debit instrument, electronic payment account, etc.), including, as applicable:
   i. Information regarding all currencies accepted by the system, the conversion rates used with each currency, and where the conversion rates are drawn from;
   ii. A clear and concise explanation of all fees;
b) As allowed by the regulatory body, any awards that are offered in the form of merchandise prizes, annuities, lump sum payments, or payment plans instead of cash payouts for each market that is offering such an award;
c) The procedures by which any unrecoverable malfunctions of hardware/software are addressed including if this process results in the voiding or cancelling of any wagers; and
d) The procedures to deal with interruptions caused by the discontinuity of data flow from the network server during an event.
e) Rules of participation, including all wagering eligibility and scoring criteria, available wagering events and markets, wager types accepted, line postings, all advertised awards, and the effect of schedule changes;
f) Payout information, including possible winning positions, rankings, and achievements, along with their corresponding payouts, for any available wager option;
g) Any non-wager purchase option and its price;
h) Any restrictive features of wagering, such as wager amounts or maximum payouts;
i) A description on prohibited or restricted persons, including any applicable limitations on wagering for restricted persons (e.g., athletes shall not wager on their team);
j) The procedures for handling incorrectly posted events, markets, odds/payouts, prices, wagers, or results;
k) A wager void and cancellation policy which shall:
   i. Include definitions and procedures for voids and cancellations involving obvious errors and material changes in circumstances for a wagering event, market, or wager selection;
   ii. Cater for wagers with multiple wagering events or markets (e.g., parlays);
   iii. Indicate any prohibitions of voiding or cancelling wagers (e.g., after a fixed time period);
l) 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;
m) For fixed odds wagering, any situations where the odds/payouts may be adjusted such as atypical winning outcomes (e.g., dead heats), cancelled legs of wagers with multiple wagering events or markets (e.g., parlays), and prorating;
n) For pari-mutual wagering, 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;
o) For live-event wagering, due to varying communication speeds or broadcast transmission latencies:
   i. Updates of the information displayed may put a player at a disadvantage to others who may have more up-to-date information; and
   ii. There may be delays incorporated in the registered time of a live-event wager to prevent past-post wagers, voids, and cancellations.

p) A statement that the operator reserves the right to:
   i. Refuse any wager or part of a wager or reject or limit wager 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;
q) If awards 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 awards (e.g., result 8-4-7);
r) The rules for any exotic wagering types (e.g., same game parlay, teaser, perfecta, trifecta, quinella, etc.) and the expected payouts;
s) What is to occur when a wagering event, market, or wager selection is cancelled or withdrawn, including the handling of selections wagers with multiple wagering events or markets (e.g., parlays) where one or more of these legs are cancelled or withdrawn;
t) How a winning wager is determined and the handling of an award in any case where a tie is possible;
u) The payment of winning wagers, including the redemption period and the method for calculation;
v) Where transactions may involve rounding, information on how these circumstances are handled shall clearly explain:
   i. Rounding up, down (truncation), true rounding; and
   ii. Rounding to what level (e.g., 5 cents).

A.4.3 Player Protection Information

Player protection information shall be approved by the regulatory body and made available to the player. The player protection information shall contain at a minimum:

a) Information about potential risks associated with excessive wagering, and where to get help for a gambling problem;
b) A statement that no underage persons are permitted to participate in event wagering;
c) A list of the available responsible gaming tools that can be invoked by the player (e.g., self-imposed limitations, time-outs, and suspensions) 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 financial 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.

NOTE: All links to problem gambling services provided by third parties are to be regularly tested by the operator. Remote wagering may not occur where the links used to supply information on player protection are not displayed or are not operational. Where the link is no longer available or not available for a significant period of time, the operator shall provide an alternative support service.

A.4.4 Terms and Conditions

A set of terms and conditions shall be approved by the regulatory body and made available to the player. The terms and conditions shall:

a) State that only individuals legally permitted by their respective jurisdiction can participate in

event 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 as required by the regulatory body;
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;
e) Clearly detail what happens to the player's pending wagers placed prior to any self-imposed or operator-imposed suspension, including the return of all wagers, or settling all wagers, as appropriate;
f) Contain information about timeframes and limits regarding deposits to and/or withdrawals from the player account, including a clear and concise explanation of all fees, if applicable;
g) State that the operator has the right to:
    i. Refuse to establish a player account for what it deems good and sufficient reason;
    ii. Refuse deposits to and/or withdrawals from player accounts for what it deems good and sufficient reason; and
    iii. Unless there is a pending investigation or player dispute, suspend or close any player account at any time pursuant to the terms and conditions between the operator and the player.

A.4.5 Privacy Policies

A set of privacy policies shall be approved by the regulatory body and made available to the player. The privacy policies shall state:

a) The PII required to be collected;
b) The purpose and legal basis for collecting and processing PII, including any specific legitimate interest relied upon by the operator or third-party service provider if required by the regulatory body;
c) The period for which PII is stored or, if no fixed period can be established, the criteria used to determine the retention period;
d) The conditions under which the PII may be disclosed and the measures used to prevent unauthorized or unnecessary disclosure;
e) The identity and contact information of the operator and the categories or identities of third-party service providers that may receive or process PII;
f) For PII collected directly from the player, whether there is a legal or contractual obligation to provide the PII and the consequences of not providing that PII;
g) Any player rights regarding their PII as required by the regulatory body;
h) Where applicable and required by the regulatory body, information regarding the use of automated decision-making, including profiling, the significance and expected consequences of such processing for the player, and any available method to contest the decision or request human review; and
i) The rights and possibility of a player to file a complaint/dispute with the regulatory body.

A.4.6 Bonusing/Promotional Offers

Players shall be able to access clear and unambiguous terms pertaining to any available bonusing/promotional offers.

a) The rules for each bonusing/promotional offer shall address the following at a minimum:
   i. The date and time the offer is presented, becomes active, and expires;
   ii. Player eligibility requirements, including any limitations on participation;
   iii. Wagering requirements and limitations, including any restrictions by wager type, wagering event and/or market;
   iv. Qualifying criteria for receiving bonusing/promotional credits and/or prizes, including any frequency of issuance;
   v. Any restriction or terms applicable to restricted bonusing/promotional credits conversions and withdrawals;
   vi. The order in which bonusing/promotional credits are used for wagers; and
   vii. How the player is notified when bonusing/promotional credits and/or prizes have been awarded;
   viii. Rules regarding offer cancellation or expiration; and
   ix. Any other offer-specific information not otherwise addressed.
b) Bonusing/promotional offers shall not be described as:
   i. "Free" unless those offers are in fact free and without any cost to the player. If the player has to risk or lose their own player funds or if there are conditions attached to their own player funds, these conditions shall be disclosed and may not be described as free; or
   ii. "Risk-free" if those offers require the player to incur a loss or risk their own player funds to use or withdraw winnings from the purportedly risk-free wager.

A.4.7 Contests/Tournaments

A contest/tournament, which permits a player to either purchase or be awarded the opportunity to engage in competitive wagering against other players, may be permitted provided the following rules are met:

a) Rules shall be made available to a player for review prior to contest/tournament registration. The rules shall include at a minimum:
   i. All conditions registered players shall meet to qualify for entry and advancement through, the contest/tournament;
   ii. Specific information pertaining to any single contest/tournament, including the available awards and distribution of funds based on specific outcomes; and
   iii. The name of the organization (or persons) that conducted the contest/tournament on behalf of, or in conjunction with, the operator, if applicable.
b) Procedures shall be in place to record the results of each contest/tournament and make publicly available for the registered players to review for a reasonable period of time. Subsequent to being posted publicly, the results of each contest/tournament shall be made available upon request. The results include the following:
   i. Name of the contest/tournament;
   ii. Dates and times of the contest/tournament;
   iii. Total number of entries;
   iv. Amount of entry fees;
   v. Total prize pool; and
   vi. Amount paid for each winning category.

NOTE: For free contests/tournaments (i.e., registered player does not pay an entry fee), the information required by the above shall be recorded except for the number of entries, amount of entry fees and total prize pool.

A.4.8 Event Wagering in Multiple Languages

Where event wagering is made available to the player in multiple language versions, the operator shall have procedures to ensure the following, as required by the regulatory body:

a) Each language version of the same wagering events, markets, and wager types shall offer the same odds/payouts and prices.
b) Each language version shall be consistent with the wagering instructions and information for that version.
c) All wagering instructions and information shall be provided in the language specified for that version.
d) Displayed terminology shall have the same meaning in all language versions, so that no version is favored or disfavored. It is not mandatory to translate common terminology used internationally for event wagering.

NOTE: If required by the regulatory body, this section will be evaluated by an independent test laboratory for the languages determined by them to be in scope.

A.5 Player Account Controls

A.5.1 Registration and Verification

If player account registration, verification, validation, and/or activation functionality is performed manually by the operator, the operator shall have processes and procedures to satisfy the requirements for "Player Account Registration and Verification" as indicated within this document.

A.5.2 Limitation to One Account per Player

The operator shall implement procedures to terminate all player accounts of any player that establishes or seeks to establish more than one account, whether directly or by use of another individual as proxy. Such procedures may allow a player that establishes or seeks to establish more than one username or more than one player account to retain one account provided that the operator investigates and makes a good-faith determination that the player's conduct was not intended to obtain a competitive advantage.

A.5.3 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 payouts associated with a fraudulent account.

A.5.4 Player Account Management

Processes and procedures shall be in place for the operator to effectuate and satisfy the requirements for "Player Account Management" prescribed in this document, including performing the following player account tasks when requested by the player or as necessary:

a) Accessing and updating a player's recorded registration information, including their PII;
b) Generating and providing a player with transaction logs or account statements;
c) Establishing and updating the authentication credentials of a player, including MFA settings or parameters;
d) Adding, modifying, and removing a player's payment methods used for financial transactions;
e) Identifying and managing inactive player accounts; and
f) Closing player accounts and handling the funds remaining in the account.

A.5.5 Player Funds Maintenance

Procedures shall be in place to ensure all financial transactions are conducted in accordance with local commerce regulations and requirements mandated by the regulatory body.

a) For financial transactions performed manually by the operator, procedures shall be in place to satisfy the requirements for "Financial Transactions" as indicated within this document.
b) The operator shall incorporate technical and procedural safeguards to prevent the acceptance of financial transactions that present elevated risk indicators.
c) A player's request for withdrawal of unrestricted player funds shall be completed by the operator within a reasonable amount of time, unless there is an unresolved player complaint/dispute or investigation. Such investigation shall be documented by the operator and available for review by the regulatory body.

A.5.6 Responsible Gaming Tools

Processes and procedures shall be in place for the operator to implement and manage responsible gaming tools, in accordance with the requirements for "Limitations, Time-Outs, and Suspensions" as indicated within this document. Additionally, the operator shall ensure that advertising or marketing materials are not sent directly to a residential address, email address, phone number, and/or any other contact method associated with a suspended player.

A.5.7 Player Account and Device Monitoring

The operator's internal control procedures shall include controls to protect player accounts and monitor player accounts, devices, and related activity to detect, investigate, and respond to unauthorized access, suspicious player activity, fraud, evasion, manipulation, or automated abuse. Such controls shall include, at a minimum:

a) Protecting player accounts containing funds from unauthorized access, changes, removal, or misuse;
b) Reviewing player transactions, including aggregated activity over time periods identified in the internal control procedures, to identify activity that triggers enhanced due diligence, reporting obligations, or other required review;
c) Identifying player accounts for investigation where account opening, account closure, deposits, withdrawals, or other activity patterns indicate potential misuse, which may include:
    i. Opening and closing accounts within short time frames; and
    ii. Deposits and withdrawals without associated wagering;
d) Detecting abnormal, inconsistent, or suspicious account, device, network, or access patterns, which may include:
    i. Rapid account creation or association of accounts with suspicious devices;
    ii. Attempts to disguise, alter, manipulate, or evade device identification or fingerprinting; and
    iii. Changes to device identity or key attributes, such as GPU, screen resolution, operating environment, hardware identifiers, or similar attributes, that may indicate device reset, data tampering, or spoofing; and
e) Procedures for using internal integrity and attestation controls as a basis for determining device trustworthiness, which may include the ability to block, restrict, or flag access from non-compliant devices where native operating system security or attestation services are unavailable, bypassed, unreliable, or compromised.

A.5.8 Player Loyalty Programs

The operator shall establish and implement controls for the administration, accounting, redemption, and disclosure of player loyalty programs or comparable benefit arrangements, where such programs are offered by the operator, and involve the use of player loyalty points or other comparable entitlements. At a minimum, the controls shall ensure that:

a) The manner in which player loyalty points or comparable entitlements are earned, accumulated, adjusted, expired, forfeited, redeemed, or otherwise used is clearly documented and available to the player;
b) Procedures to ensure that awards, benefits, or redemption opportunities are equally available to all players who achieve the minimum level of qualification for such player loyalty points or other comparable entitlements.
c) Redemption of player loyalty points or other comparable entitlements earned are performed as a secure transaction that automatically debits the balance for the value redeemed;
d) All transactions involving player loyalty points or other comparable entitlements are recorded, including points earned, redeemed, adjusted, expired, forfeited, or reversed; and
e) Player loyalty point or other comparable entitlement balances and related transaction history are made available to the player upon request.

A.6 Wagering Procedures and Controls

A.6.1 Wagering Events, Odds/Payouts, and Outcome Management

The operator shall establish and maintain documented procedures governing the lifecycle of wagering events, markets, odds/payouts, and outcomes, ensuring integrity, accuracy, transparency,

and compliance with applicable laws. These procedures shall be based on the respect of integrity, responsible gaming, and ensuring transparency, and shall provide coverage for:

a) Ensuring that each wagering event, market, and wager type offered for wagering meets the following criteria:
   i. The wagering event or market result can be documented and verified;
   ii. The wagering event or market result can be generated by a reliable and independent process;
   iii. The wagering event or market result is not likely to be affected by any wagers placed;
   iv. The wagering event is effectively supervised by a sports governing body or equivalent which shall, at minimum, prescribe final rules and enforce codes of conduct that include prohibitions on wagering by insiders;
   v. The wagering event can be conducted in a manner that ensures sufficient integrity monitoring controls exist so that the outcome may be trusted; and
   vi. There are integrity safeguards in place which are sufficient to mitigate the risk of match-fixing, cheat-at-play, and other illicit activity that might influence the outcome of the wagering event.
b) Setting and updating the odds/payouts and prices including:
   i. Publicly providing the current odds/payouts and prices;
   ii. Changing odds/payouts and prices as necessary to handle exceptions; and
   iii. Properly logging and periodically logging the odds/payouts and prices.
c) Monitoring all changes to odds/payouts, prices, market availability (including suspensions or blocking), and significant movements or fluctuations throughout a wagering event.
d) Validating the accuracy of wagering data and outcomes and implementing controls to detect and prevent fraudulent or manipulative activities.

A.6.2 Statistics/Line Data

The operator or a third-party statistics/line service provider shall ensure that any statistics/line data that is made available to the player pertaining to a wagering event or market uses a data source allowed by the regulatory body and is kept reasonably accurate and updated. As required by the regulatory body, controls shall be implemented for the operator to review and ensure that the data source and corresponding statistics/line data:

a) Are complete, accurate, reliable, timely, and available;
b) Are appropriate to provide the outcome for the wagering events, markets, and wager types for which it is used; and
c) Meet any other conditions considered appropriate by the regulatory body.

NOTE: The regulatory body may require a statistics/line service provider to undergo an independent third-party evaluation against industry standards for statistics/line data, such as the International Betting Integrity Association (IBIA) Data Standards, or other requirements as required by the regulatory body.

A.6.3 Live-Event Wagering

There shall be documented procedures to ensure and monitor the integrity of the live-event wagering offerings, the outcome handling and player protection. These procedures shall address:

a) Timing and validation of outcome information, including appropriate delays and changes; and
b) Mitigation of courtsiding or information asymmetry (e.g., use of latency or buffering mechanisms).

A.6.4 Suspending Wagering Events and Markets

There shall be established procedures for manually suspending wagering events and markets (i.e., stop accepting wagers for that market or markets associated with that wagering event).

A.6.5 Managing Risk

The operator shall use mechanisms that offset loss or manage or layoff risk in the operation of event wagering, including through layoff wagers, liquidity pools, exchanges, or similar mechanisms in another approved jurisdiction in which the operator's event wagering is offered if adequate protections are continuously maintained to ensure sufficient funds are available to pay winnings. The operator placing a layoff wager shall inform the operator accepting the wager that the wager is being placed by an operator and shall disclose their identity.

A.6.6 Wager Voiding and Cancellation Procedures

Wagers cannot be modified except to be voided or cancelled as provided for in the operator's published wager void and cancellation policy. The following requirements apply to wager voids and cancellations:

a) Player initiated voids and cancellations may be authorized in accordance with the void and cancellation policy. An operator may offer players a grace period to request a void or cancellation of their wager, provided that such grace period shall end before a wagering event has begun.
b) Operator initiated voids and cancellations shall provide a reason for the void or cancellation to a player (e.g., past-post wager). An operator shall not void or cancel any wager after the outcome of an event is known without the prior approval of the regulatory body.
c) If a wager is declared voided or cancelled, the wager shall be refunded to the player.

A.6.7 Wagering Period Controls and Past-Post Prevention

The operator shall maintain documentation, procedures, and controls describing how wagering periods are controlled and how past-post wagers are prevented. Such documentation, procedures, and controls shall include, at a minimum:

a) The method used to open, close, or suspend wagering periods, including any period in which wagers are unable to be placed, such as while odds/payouts or prices are being updated;
b) The method used to identify and prevent wager acceptance after the applicable wagering period is closed; and
c) Where these functions are managed or supported by a third-party service provider, the provider's role and the technical or internal control procedures used by the operator to verify that wagering periods and past-post prevention controls are operating as intended.

A.6.8 Results Verification and Settlement

Prior to settlement, there shall be a policy for the confirmation of wagering event and market outcomes. Procedures shall ensure that:

a) Outcomes are verified based on qualified and approved data sources, including where verification or settlement is automated or supported by an external feed;
b) Where an external feed is used, contingency controls are in place for cases where access to the external feed is unavailable, and the operator verifies, either technically or through internal control procedures, that outcomes are received, processed, and settled as intended; and
c) Corrections in outcomes, including statistical or official changes, are properly managed, controlled, and auditable.

A.6.9 Settled or Redeemed Wager Payment

In the event of a failure of the Event Wagering System's ability to pay settled or redeemed winning wagers, the operator shall have controls detailing the method of paying these wagers when such system failures cannot be resolved in a timely fashion.

A.6.10 Retail Wagering Operations

The following procedures shall be in place for retail wagering operations within the Wagering Venue:

a) Procedures to describe the operations and the servicing of Retail Wagering Terminals, including the handling of error conditions and performing reconciliations;
b) Procedures to ensure accessibility requirements observed by the regulatory body are met for the installation of Self-Service Wagering Terminals.
c) Procedures for wager transactions using an OTC Wagering Terminal, 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 PII 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; and
d) Procedures for handling cancelled wagering events and withdrawn wager selections for wagers with multiple wagering events or markets (e.g., parlays), including providing refunds to players who were not refunded automatically by the system (e.g., wagers placed anonymously).

A.6.11 Sponsored Players for Peer-to-Peer (P2P) Wagering

The operator shall have processes to ensure the player is not disadvantaged by sponsored players participating in P2P wagering. The following risks are expected to be mitigated:

a) The operator's controls shall mitigate the conflict between the role of the sponsored player and the role of authorized personnel who have access to the Event Wagering System (both physically and virtually) to be able to manipulate the wagers or have information not available to all the

other players and be able to take advantage of it;
b) The operator shall not profit from the P2P wagering participation (beyond the rake, commission, or fee);
c) If the sponsored player's wager is funded by the operator, the sponsored player shall not profit from the P2P wagering participation, the funds may not be withdrawn, and so shall ultimately be lost/wagered; and
d) Procedures shall be in place to address the risk that the sponsored player is motivated to protect personal wagers beyond the assignment of stimulating P2P wagering participation. If the sponsored player risks private wagers, then the sponsored player shall not have any knowledge of software or other PII (the sponsored player is a bona fide independent contractor with no prior relationship with the operator).

A.7 Integrity, Collusion, Fraud, and AML/ATF Controls

A.7.1 Integrity and Compliance Program

The operator shall implement and maintain documented policies, procedures, controls, and monitoring mechanisms designed to ensure the integrity of event wagering and comply with anti-money laundering (AML) and anti-terrorist financing (ATF) obligations. Such policies, procedures, controls, and mechanisms shall be periodically reviewed and updated as necessary based on operational experience, regulatory requirements, identified risks, and environmental changes.

A.7.2 Integrity Monitoring and Response

The operator shall establish procedures to monitor wagering, markets, player accounts, transactions, player communications where available, devices, and related activity for suspicious player activity, coordinated player activity, prohibited player activity, unauthorized player assistance, and other integrity concerns. Such procedures shall provide for the review, investigation, escalation, and appropriate response to detected or reasonably suspected integrity concerns, and shall include, at a minimum:

a) Review and investigation of alerts, reports, complaints, or other indications of integrity concerns;
b) The ability to refuse, delay, suspend, void, cancel, or limit wagers, wagering activity, transactions, or player account activity, where permitted by the regulatory body, internal control procedures, or wagering rules;
c) The ability to restrict, suspend, or close player accounts where integrity concerns are identified or reasonably suspected;
d) Documentation of the basis for any material action taken; and
e) Escalation of confirmed or suspected integrity concerns to appropriate internal personnel and, where required, to the regulatory body or other appropriate authority.

A.7.3 Regulatory Notification and Reporting

Unless otherwise directed by the regulatory body, the operator shall document and notify the regulatory body upon detecting or becoming aware of:

a) Any suspected illegal, criminal, fraudulent, or prohibited activity related to event wagering that is required to be reported to the regulatory body;
b) Any person suspected of misrepresenting their identity or using false identification to establish or attempt to establish a player account or place a wager;
c) Any criminal or disciplinary proceeding commenced against the operator in connection with its event wagering operations;
d) Any activity, pattern, or conduct that raises a concern regarding the integrity of a wager, wagering event, or event wagering generally; and
e) Any other matter required to be reported by the regulatory body, internal control procedures, or applicable laws or regulations.

A.7.4 Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF)

The operator shall develop, implement, and maintain AML/ATF policies and procedures that adequately address the risks posed by event wagering for potential money laundering and terrorist financing. Such policies and procedures shall include, at a minimum:

a) Internal control procedures designed to ensure ongoing compliance with applicable AML/ATF laws, regulations, and standards recognized or required by the regulatory body;
b) Ongoing training of relevant personnel in the identification, handling, escalation, and reporting of unusual and suspicious transactions or activities;
c) Designation of one or more responsible individuals for AML/ATF compliance, including responsibility for reporting unusual or suspicious transactions and activities to appropriate authorities;
d) Use of automated systems, monitoring tools, and data processing methods to support AML/ATF monitoring, detection, investigation, and reporting; and
e) Periodic independent testing of AML/ATF policies and procedures at a scope and frequency required by the regulatory body, with records of such testing maintained.

A.7.5 Recordkeeping

The operator shall maintain complete, accurate, and auditable records demonstrating compliance with this section, including monitoring activity, alerts, reports, investigations, decisions, actions taken, regulatory notifications, AML/ATF documentation, and other supporting evidence necessary to demonstrate compliance.

A.8 Geolocation Solution Controls

A.8.1 Geolocation Solution Audits

The geolocation service provider shall, where required by the regulatory body, allow periodic audits to assess and measure the Geolocation Solution's continued ability to reasonably detect and mitigate existing and emerging location fraud risks, including the operational procedures and controls within this section, as well as the "Geolocation Operations and Enforcement" section within this document.

A.8.2 Geolocation Accuracy Radius

To ensure location data is accurate and reliable, the geolocation service provider shall ensure that Geolocation Solution:

a) Calculates and applies an appropriate accuracy radius for each geolocation check based on authenticated location data sources and relevant risk factors, which may include internet connection type, mobility risk, proximity to permitted geofence borders, and velocity considerations;
b) Reasonably determines whether the player's real-world geographic location, inclusive of the accuracy radius, is contained within the permitted geofence; and
c) Provides configurable controls for determining whether the accuracy radius of the location data sources may overlap or exceed buffer zones established for the permitted geofence.

A.8.3 Geolocation Mapping

The geolocation service provider shall have procedures to reasonably mitigate and account for discrepancies between mapping sources and variances in geospatial data. This may include utilizing boundary polygons based on accurate maps and overlaying location data onto these boundary polygons.

A.8.4 Geolocation Solution Maintenance

To maintain the overall integrity of the Geolocation Solution, the geolocation service provider shall ensure the Geolocation Solution:

a) Utilizes closed-source databases (IP, proxy, VPN, fraud, etc.) that are frequently updated and periodically tested for accuracy and reliability;
b) Undergoes frequent updates, including configuration changes and the application of patches, to maintain cutting-edge data collection, device compatibility, and fraud prevention capabilities against potential data manipulation techniques and location fraud risks (e.g., fake location applications, virtual machines, remote desktop programs, etc.); and
c) Utilizes dynamic cryptographic signing to verify that all geolocation payloads originate exclusively from an authorized and untampered instance of the provider's Software Development Kit (SDK), ensuring the authenticity of the location data source and preventing the use of harvested keys, 'headless' clients, or unauthorized library emulations.

A.8.5 Geolocation Fraud Monitoring

Given that location fraud shall be assessed based on individual geolocation checks and cumulative player location activity over time, the geolocation service provider shall employ mechanisms to:

a) Actively assess the risk profile of each player and device using current and historical geolocation access data and reasonably detect suspicious player activity or location anomaly indicators;
b) Provide alerting mechanisms to reasonably identify unauthorized or improper access, fraudulent activity, and players or devices that have been blocked or otherwise flagged for investigation; and
c) Cumulatively aggregate, authenticate, and analyze historical geolocation and fraud data to support investigations of players or devices that exhibit suspicious player activity or location anomaly indicators.

A.8.6 Geolocation Reporting and Analytics

The geolocation service provider shall have procedures to maintain and provide the operator and regulatory body with a real-time dashboard and data feed of all geolocation checks which:

a) Is customizable and displays location data and visuals on demand;
b) Displays and is filterable by, at a minimum, the following data, as applicable:
   i. Time period;
   ii. Anonymized player ID;
   iii. Relevant location information (e.g., device ID, location data, connection type, etc.); and
   iv. Geolocation result including the reason for any geolocation failure.
c) Provides an interactive mapping tool capable of:
   i. Displaying locations of geolocation checks; and
   ii. Using coordinates to pinpoint locations.
d) Provides data, visuals and reporting capabilities pertaining to suspicious or unusual activities, including:
   i. Malicious or repeated location spoofing;
   ii. Account sharing, and device sharing;
   iii. Inconsistent locations (location jumping); and
   iv. Other high-risk transactional data.

A.8.7 Operator Responsibilities for Geolocation

The operator shall maintain documented policies and procedures related to the use of Geolocation Solutions.

a) The operator shall have a process in place to verify that the latest versions of the Geolocation Solution are being used.
b) The operator shall receive alerts or notifications when Geolocation Solution updates or patches become available.
c) Where a secondary Geolocation Solution is used, the operator shall maintain documented criteria, approved by the regulatory body, defining the specific circumstances under which the secondary Geolocation Solution may be utilized (e.g., primary Geolocation Solution outage). For switching Geolocation Solutions, the operator shall:
   i. Maintain logs or reports documenting when switching occurred and the corresponding reason for each switch; and
   ii. Periodically review switching events to ensure they align with the documented criteria.
d) Where the operator utilizes any internal geolocation logic prior to submitting requests to Geolocation Solutions, this logic shall be formally documented, approved, and designed in a manner that does not compromise regulatory requirements.

Appendix B: Integrity and Security Assessments

B.1 Introduction

B.1.1 General Statement

Unless otherwise specified by the regulatory body, integrity and security assessments shall be conducted against the applicable controls and tests identified in the GLI Gaming Security Framework (GLI-GSF) and any other controls and tests identified by the regulatory body. The integrity and security assessments consist of a Gaming Information Security (GIS) Controls Audit and a Gaming Technical Security (GTS) Assessment of the critical components of the Event Wagering System's gaming production environment, including but not limited to:

a) Components which record, store, process, share, transmit, or retrieve sensitive information (e.g., personally identifiable information (PII), financial transactions, authentication credentials, encryption keys, validation numbers, outcomes, etc.);
b) Components which receive or process statistics/line data used to determine the odds/payouts and outcomes of wagering events and markets;
c) Components which store results or record the current state of a player's wagering activity;
d) Points of entry to and exit from the above critical components (other systems and interfaces which provide access to or communicate directly with the above critical components); and
e) Communication networks which transmit sensitive information.

NOTE: It is recommended for the regulatory body to allow flexibility for integrity and security assessment schedules for multi-jurisdictional operators to allow consolidation of assessments for multiple jurisdictions to a common schedule. Please refer to the *GLI Gaming Security Framework (GLI-GSF)* for additional information.

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 house 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.

Attendant Interface – An interface application or program through which the attendant views and/or interacts with the OTC Wagering Terminal.

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.

Automated Decision-Making – The ability to make decisions by technological means based on PII or data provided directly by players, data observed about players, or derived or inferred data (e.g., risk rating). For any type of processing to be classed as automated rather than solely automated, there will be meaningful human involvement in the process (e.g., through review or filtering) and that human involvement will take place prior to the final decision.

Back – To wager on a wager selection occurring (wagering that an outcome will occur) in a given market.

Backup – A copy of files and programs made to facilitate recovery if necessary.

Barcode – An optical machine-readable representation of data, including interleaved 2 of 5 barcodes, quick response (QR) codes, or any machine-readable codes 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.

Beacon Technology – Short-range communications technology used to assist in determining whether a Remote Player Device is within a permitted geofence. Examples include Bluetooth Beacons, Near Field Communication, Ultra-Wideband, Ultrasonic Signals, or comparable technologies.

Biometric – A biological identification input, such as fingerprints or retina patterns.

BT, *Bluetooth* – A low power, short-range wireless communications protocol utilized for the interconnection of cellular phones, computers, and other electronic devices. Bluetooth connections typically operate over distances of ten meters or less and rely upon short-wavelength radio waves to transmit data over the air.

Bonusing/Promotional Offers (aka "Bonusing/Promotional Credits and/or Prizes" or "Bonusing/Promotional Amounts") – Credits and/or prizes not included in the standard odds/payouts for a market, that are awarded based upon pre-determined events or criteria established by the terms of the offers. Such offers may be triggered by player activity tied to a specific player account or wager, or by external conditions not directly tied to player activity. Examples include earning restricted bonusing/promotional credits based on a first deposit or wager, awarding prizes for a certain amount wagered on a wagering event or market; awarding credits for wagering more than a certain amount within a specific time period; multiplying all wins within a specified range by a specified value.

Cancelled Wager – A wager that was valid at the time that it was made but has since been invalidated in a manner acceptable by the regulatory body due to an event or action that prevents its completion.

Client-Side Tampering – The unauthorized manipulation of location data, application logic, or related client-side components before a geolocation request is communicated from the Remote Player Device to the Event Wagering System and/or Geolocation Solution.

Communications Technology – Any method used, and the components employed, to facilitate the transmission and receipt of information, including transmission and reception by systems using wire, wireless, cable, radio, microwave, light, fiber optics, satellite, or computer data networks, including the Internet and intranets.

Coordinated Player Activity – Activity involving two or more players, accounts, devices, payment methods, chat or external communication channels, or related identifiers that may indicate collusion, multi-accounting, syndicate behavior, shared account control, information sharing, signaling, complementary or offsetting wagers across related markets, or other conduct designed to obtain an unfair advantage, evade controls, or compromise the integrity of event wagering.

Coupon – A wagering instrument that is used primarily for promotional purposes and which can be redeemed for restricted or unrestricted bonusing/promotional 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.

Debit Instrument – A card, code, or other device with which a person may initiate an electronic funds transfer. The term includes, without limitation, a prepaid access instrument.

Discretionary Account Funds – Restricted bonusing/promotional credits and bonusing/promotional credits that have a possible expiration.

Dividend – The payout amount per unit wager payable to a winning pari-mutuel wager.

Domain – A group of computers and devices on a network that are administered as a unit with common rules and procedures.

EFT, *Electronic Funds Transfer* (aka "ECT", "Electronic Credits Transfer") – A financial transaction involving an electronic transfer of funds between an electronic payment account and a player account using a financial service provider. This includes Automated Clearing House (ACH) transfers.

Electronic Payment Account – An account maintained with a financial institution or third-party financial service provider, such as PayPal, Google Pay, or Apple Pay, for the purposes of making electronic funds transfers. The term does not include a player account, or any other account held by an operator and used for wagering purposes.

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 Wagering – The offering, placement, and acceptance of wagers on one or more wager selections within markets associated with a wagering event, including the determination and settlement of such wagers in accordance with the established conditions, rules, and odds/payouts.

Event Wagering System – The hardware, software, firmware, communications technology, other equipment, as well as operational procedures implemented in order to allow player participation in event wagering, and, if supported, the corresponding equipment related to the display of 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, disable wagering events, generate various wager transaction, financial transaction, and player account reports, input outcomes for wagering events, and set any configurable parameters. The term does not include Remote Player Devices or communications technology used by a player to participate in remote wagering.

Exchange Wagering – A form of P2P wagering in which two or more players place identically opposing wagers, allowing players to wager on both winning and non-winning outcomes in the same wagering event or market.

Exchange Wagering Liquidity – The amount of unmatched exchange wagering volume available at specific odds/payouts in a market, indicating how easily a player's wager can be matched.

Financial Service Provider (aka "Payment Processor") – An in-house or third-party entity who directly facilitates payment processing, including the depositing of funds to or withdrawing of funds from player accounts.

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 Wagering – A wager category 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 Bet/Demo Mode – A wager mode that allows a player to simulate wagering without placing any paid wager, principally for the purpose of learning or understanding wagering mechanics.

Geolocation Information Leakage – The exposure of validation logic, diagnostic feedback, rejection codes, technical failure reasons, or other information that could enable a player or unauthorized party to understand, bypass, or evade geolocation controls.

Geolocation Integrity Risk – Any attack, vulnerability, or unauthorized interference with location data, geolocation results, and related geolocation controls. These may include, but are not limited to, replay attacks, "Man-in-the-Middle" attacks, geolocation result forgery/reconstruction, geolocation information leakage, client-side tampering, Wi-Fi injection, or similar methods.

Geolocation Result Forgery/Reconstruction – The generation or alteration of apparently valid geolocation results through reverse engineering, exposed software development kit (SDK) logic or validation methods, unauthorized interfaces, manipulated client-side components, or similar exploits.

Geolocation Service Provider – An in-house or third-party entity who identifies, or provides information for the identification of, the real-world geographic location of individuals.

Geolocation Solution – A mechanism to reasonably detect the real-world geographic location of a player when using their Remote Player 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.

Inactive Player Account – A player account considered to be inactive under the conditions as specified in the terms and conditions.

Identically Opposing Wagers – Wagers in which one or more players offer to lay a wager selection at the same odds/payout at which one or more players offer to back that same outcome, with the amount subject to the lay being proportionately commensurate to the amount subject to the back.

Incrementing Bonus Jackpot – A monetary award or “jackpot payoff” that increases on the occurrence of one or more specific conditions established by the wagering rules. In addition to those

specific conditions, it is acceptable for incrementing bonus jackpots to also increase according to the amounts wagered.

Information Security – Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability

Internet – An interconnected system of networks that connects computers around the world via TCP/IP.

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 operator or software supplier to allow the installation of unauthorized software.

Key – A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification.

KYC Service Provider, *Know-Your-Customer Service Provider* (aka "Identity Verification Service Provider") – An in-house or third-party entity who verifies, or provides information for the verification and validation of the identity of individuals.

KYC Solution, *Know-Your-Customer Solution* (aka "Identity Verification Solution") – A mechanism to reasonably verify and validate the identity of individuals.

Lay – To wager on a wager selection not occurring (wagering the outcome will not occur) in a given market.

Layoff Wager – A wager placed by an operator with another operator to offset liability.

Location Anomaly Indicator – Any current or historical geolocation pattern that may indicate suspicious, unauthorized, coordinated, automated, or improper access. These may include, but are not limited to, impossible travel, anomalous velocity, successive physical locations that could not reasonably be traveled between in the time reported, location behavior inconsistent with account, device, or network history, repeated failed or unauthorized geolocation attempts, or patterns suggesting coordinated, relayed, shared, or automated access activity.

Line Posting – A value that establishes a wager's potential payout (e.g., moneyline + 175) or the conditions for a wager to be considered a win or loss (e.g., point spread + 2.5).

Link Utilization – The percentage time that a communications link is engaged in transmitting data.

Live-Event Wagering (aka "In-Play Wagering" or "In-Game Wagering") – A wager category in which wagers are accepted on a wagering event while the event is in-progress or taking place.

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 – The unauthorized interception, modification, injection, substitution, or manipulation of location data or geolocation results while communicated between the Remote Player Device, the Event Wagering System, and/or the Geolocation Solution.

Market – A proposition within a wagering event that specifies the outcomes upon which one or more wager selections may be offered, including the applicable conditions, settlement criteria, and odds/payouts (e.g., match winner, total points, player performance).

Market Maker – An entity who provides exchange liquidity and/or odds/payouts to an operator that is offering exchange wagering.

Matched Wager – A wager that is formed when two or more players are confirmed as having placed identically opposing wagers in a given market.

MFA, *Multi-Factor Authentication* – A type of authentication which has been demonstrated to effectively provide higher security than a username and password alone to verify an individual's identity. Supporting technologies may include Customer Identity and Access Management (CIAM) platforms, Fast Identity Online (FIDO) authentication solutions, or similar authentication frameworks.

Moneyline – A wager type in which the player wagers on which participant will win a wagering event, without the application of a point spread or handicap.

NFC, *Near Field Communication* – A short-range wireless connectivity standard that uses magnetic field induction to enable communication between devices when they are touched together or brought within a few centimeters of each other.

Non-Wager Purchase – A purchase made by the player that debits the funds available for wagering and which is used for entertainment purposes only. A non-wager purchase does not influence the outcome of the wager.

Operator – A person or entity that oversees event wagering, using both the technological capabilities of the Event Wagering System as well as their own internal control procedures. For the purposes of this document, the term operator also includes any person or entity that oversees some or all event wagering on the operator's behalf, such as a wagering venue manager, software supplier, or a management services provider.

OTAC, *One-Time Authentication Credential* (aka "One-Time Passcode (OTP)") **–** A secure, temporary, authentication credential either sent to a Remote Player Device, or an email address, or phone number that has been confirmed as being owned or possessed by the player or generated by an authentication application or software program used by the player and accepted by the Event Wagering System.

OTC Wagering Terminal, *Over-the-Counter Wagering Terminal* – 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 and, if supported, may be used for redemption of wager records and other authorized activities.

Over/Under (aka "Total Wager") – A wager type in which the player wagers on whether the combined total of a specified statistic or scoring measure, such as total points, goals, runs, or rounds, will be greater than or less than the total posted by the operator.

P2P Wagering, *Peer-to-Peer Wagering* – A wager category where players wager with and against one another rather than against the operator, who may take a rake, commission, or fee for facilitating the wagering activity. Examples of P2P wagering include, but are not limited to, exchange wagering, head-to-head wagering, contests, tournaments, pools, etc.

Pari-Mutuel Wagering – A wager category where individual wagers are gathered into a pool. The winnings are calculated by sharing the pool among all winning wagers.

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 a wagering event.

Passkey – An authentication credential that uses a pair of cryptographic keys and typically authenticates an individual through biometrics, a PIN, or device authentication.

Password – An authentication credential, using 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).

Pending Wager – A wager or portion of a wager placed in a given market that does not become part of a matched wager because there are not one or more available exchange wagers in that market with which to form one or more identically opposing wagers.

Peripheral – An internal or external device connected to Retail Wagering Terminal that supports credit acceptance, credit issuance, player interaction, or other specialized functions.

Perfecta (aka “Exacta”) – A wager type in which the player picks the first and second place participants in a wagering event in the correct finishing order.

Permitted Geofence – A virtual geographic perimeter delineated by a Global Positioning System (GPS), Radio-frequency Identification (RFID), or other similar technology, within which the player may place a wager and/or perform account activities as required by the regulatory body.

PII, *Personally identifiable information* – Sensitive information that identifies, relates to, describes, or can reasonably be linked to a player, including, but not limited to, a player’s full legal name, date

of birth, residential address, contact information, full or partial government identification number (e.g., driver's license number, social security number, taxpayer identification number, passport number, or equivalent), personal financial information (e.g., credit or debit instrument numbers, bank account numbers, etc.), or other personal information as may be specified by the regulatory body.

PIN, *Personal Identification Number* – An authentication credential, using a numerical code associated with an individual and which allows secure access to a domain, account, network, system, etc.

Player Account (aka "Wagering Account") – An account maintained by an operator for a player where information relative to wager 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 electronic payment account, or an account used solely by an operator to track bonusing/promotional points or credits or similar benefits issued by an operator to a player which may be redeemed for merchandise and/or services.

Player Account Manager – The hardware, software, firmware, communications technology, other equipment, as well as operational procedures used to create, manage, and track player accounts and history, and to provide player account functions, including account management, payments, wallets, and responsible gaming controls. The Player Account Manager may be a standalone system or integrated within another part of the Event Wagering System.

Player Application – The software used to take part in wagers and financial transactions with the Event Wagering System which, based on design, is downloaded to or installed on the Remote Player Device, run from the Event Wagering System which is accessed by the Remote Player Device, or a combination of the two. Examples of Player Applications include proprietary download software packages, html, flash, etc.

Player Attribute – Any specific and verifiable fact concerning a player or group of players which is based upon objective criteria relating to the player or group of players and which may be utilized to affect some prescribed change to a wager configuration.

Player Interface – An interface application or program through which the individual views and/or interacts with the Remote Player Device or Self-Service Wagering Terminal to communicate their actions to the Event Wagering System.

Player Loyalty Program – A program that awards player loyalty points (or other comparable entitlement) to players, typically based on the volume of play or revenue received from a player.

Point Spread – A wager type in which a handicap, expressed as a number of points, goals, runs, rounds, or other scoring measure, is applied to one or more participants for wagering purposes.

Pool – An accumulated reservoir of monetary contributions.

Printer – A Wagering Terminal peripheral that prints wager records and/or wagering instruments.

Prepaid Access Instrument – A card, code, electronic serial number, mobile identification number, personal identification number or similar device used in conjunction with an Event Wagering System that allows player access to funds that have been paid in advance and can be retrieved or transferred at some point in the future through such a device.

Profiling – Any form of automated processing of PII consisting of the use of PII gathered from various sources to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's economic situation, personal preferences, interests, reliability, behavior, location, etc.

Progressive Jackpot – A monetary award or "jackpot payoff" that increases generally based on a function of wagers or some other metrics.

Prohibited Player Activity – Activity prohibited by internal control procedures, wagering rules, or applicable laws or regulations. These may include, but are not limited to, cheating, fraud, theft, embezzlement, collusion, identity misrepresentation, money laundering, terrorist financing, use of funds derived from illegal activity, unauthorized player assistance, or other activity that compromises the integrity of event wagering.

Proposition Wager (aka "Prop Bet") **–** A wager type in which the player wagers on the occurrence or non-occurrence of a specific outcome of events within a wagering event not directly involving the wagering event's final outcome.

Protocol – A set of rules and conventions that specifies information exchange between devices, through a network or other media.

Proxy – 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.

Quinella – A wager type in which the player picks the first and second place participants in a wagering event, but not necessarily in the finishing order.

Rake, Commission, or Fee – An amount retained and not distributed by the operator from the total amount wagered on a wager selection.

Remote Player 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 Player Device include a personal computer, mobile phone, tablet, etc.

Remote Wagering – Event wagering conducted using Remote Player Devices on an in-venue wireless network or over the internet, depending on the implementations authorized by the regulatory body.

Replay Attack – The capture and reuse of previously valid location data, geolocation results, or successful geolocation checks to falsely satisfy a subsequent geolocation check.

Restricted Bonusing/Promotional Credits (aka "Non-Cashable Bonusing/Promotional Credits") – Bonusing/Promotional amounts that either are not redeemable for cash or cannot be cashed out until a wagering requirement or other restrictions associated with the credits is met.

Restricted Player Funds – Player funds that are not redeemable for cash, including restricted bonusing/promotional credits.

Retail Wagering – Event wagering conducted using Retail Wagering Terminals located within a Wagering Venue.

Retail Wagering Terminal – 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.

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 Player Device or install software that the operator or software supplier would not allow to be installed.

Secure Communication – Communication that provides the appropriate confidentiality, authentication, and content integrity protection.

Self-Service Wagering Terminal – 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 wager records and other authorized activities.

Sensitive Information – Information that shall be handled in a secure manner, such as PII, wagering data, validation numbers, authentication credentials, PINs, passwords, secure seeds and keys, and other data which is of a sensitive nature.

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 Remote Player Devices.

Single-Game Wager – A wager type in which the player wagers on a single wagering event, rather than on multiple wagering events.

Source Code – A text listing of commands to be compiled or assembled into an executable computer program.

Sponsored Player (aka "Proposition Player" or "Shill") – A player hired by the operator or other entity to participate in event wagering, and wagers using personal funds or funds provided directly or indirectly by the operator or other entity.

Straight Wager – A wager type in which the player wagers on a single wager selection that is not combined with any other wager selection for payout purposes.

Suspicious Player Activity – Activity, pattern, or condition involving wagering, markets, player accounts, transactions, communications, devices, or related activity that may indicate coordinated player activity, unauthorized player assistance, prohibited player activity, unauthorized proxy betting, or other integrity concerns. These may include, but are not limited to, irregular wagering patterns or series of abnormal wagers or wagering activity, unusual wagering volumes, wager structuring, timing anomalies, rapid changes in wagering behavior, material swings or changes in odds/payouts or prices, market suspensions, match-fixing or wagering event manipulation, misuse of insider information, abuse of bonusing/promotional offers, payment fraud, identity theft, account takeover or misuse, or behavior inconsistent with normal player activity.

Teaser – A wager type that combines two or more wager selections, typically involving point spreads or over/unders, in which the player receives an adjusted spread or total for each selection in exchange for reduced odds or payout.

Third-Party Service Provider – An entity who acts on behalf of an operator to provide services used for the overall conduct of event wagering.

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 player input device by using electrical touch point locations on the display screen.

Tournament (aka "Contest/Tournament") – An organized, measured event that permits a player to engage in competitive wagering against other players. An out-of-revenue tournament involves only non-wagered competition using tournament credits or points that have no cash value. In contrast, an in-revenue tournament allows for wagered competition in conjunction with the operation of the tournament.

Trifecta – A wager type in which a player wins by selecting the first, second, and third place participants in a wagering event in the correct finishing order.

Unauthorized Access – A person gains logical or physical access without permission to a network, system, application, data, or other resource.

Unauthorized Player Assistance – The use of bots, scripts, and other unauthorized player software, which may include, automated tools, external systems, real-time analytical tools, or prohibited decision-making aids to generate, recommend, execute, or influence wagers or wagering strategies in violation of the wagering rules.

Unrestricted Bonusing/Promotional Credits (aka "Cashable Bonusing/Promotional Credits") – Bonusing/Promotional amounts that are redeemable for cash.

Unrestricted Player Funds – Player funds that are redeemable for cash, including unrestricted bonusing/promotional credits.

Virtual Event Wagering – A form of wagering that allows for the placement of wagers on computer-generated simulations of, or previously recorded, wagering events in which virtual participants compete with one another.

Virtual Opponent – A computer-based player that participates in P2P wagering and effectively mimics the actions of a live player.

Virtual Participant – The athlete or other entity that competes in a virtual wagering 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.

Voided Wager (aka "Void Wager") **–** A wager that was not valid at the time it was placed or a wager that was valid at the time it was placed but has since become invalid for reasons, including but not limited to the change in eligibility status of a participant or subject of the wager.

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 (aka "Bet") **–** Any commitment of value by a player on wager selections within markets associated with a wagering event.

Wager Category – A high-level classification of wagers based on how odds are established, how players interact, and how payouts are determined, describing the underlying wagering model rather

than the specific market offered. Examples include fixed odds wagering, pari-mutuel wagering, exchange wagering, wagering pools, live-event wagering, and any other category of wagering approved by the regulatory body. A single wager may fall within multiple categories depending on its characteristics (e.g., a live-event wagering fixed odds wager).

Wager Record (aka "Wagering Ticket" or "Betslip") **–** A printed ticket or electronic message confirming the acceptance of one or more wagers.

Wager Selection – A specific outcome or option chosen by the player within a market upon which a wager is placed. A wager selection represents the player's prediction of the result of a market and forms the basis for determining the outcome and settlement of the wager (e.g., Team A to win, over 2.5 goals, a specific player to score).

Wager Type – A specific form or instance of a wager within a wager category, determined by the particular outcome, condition, or structure of the wager, including how one or more wager selections are combined, evaluated, and settled across one or more markets. Wager types include, but are not limited to single-game wagers, teasers, moneyline, point spreads, over/under, win/place/show, perfecta, trifecta, quinella, parlays, proposition wagers, straight wagers, and any other type of wagers approved by the regulatory body.

Wagering Event – A sporting event or game, competition, contest, match, race, or other occurrence or type of activity approved by the regulatory body upon which wagers may be offered.

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 device and the Retail Wagering Terminal which is used for credit insertion and redemption.

Wagering Platform (aka "Betting Server" or "Wager Aggregator") – The hardware, software, firmware, communications technology, other equipment, as well as operational procedures used to host event wagering and/or aggregate wagering content, as well as drive the features common to wager offerings, wager configurations, data sources, reporting, etc. The Wagering Platform may be a standalone system or integrated within another part of the Event Wagering System.

Wagering Pools – A wager category where players contribute to a common prize pool, and payouts are determined based on the distribution of the pool among winning players, often relative to the number of correct selections or rankings.

Wagering Rules (aka "House Rules") – Any written, graphical, and auditory information compiled by the operator for the purpose of summarizing portions of the internal control procedures and certain other information necessary to inform the public of the functionality of the event wagering operations.

Wagering Venue – A physical location or site where retail wagering activities take place, such as casinos, racetracks, off-track-betting parlors, gaming halls, or other similar facilities where Retail Wagering Terminals are installed.

Wi-Fi – The standard wireless local area network (WLAN) technology for connecting computers and electronic devices to each other and/or to the internet.

Wi-Fi Injection – The use of synthetic, spoofed, replayed, or otherwise manipulated Wi-Fi signals or access point data to falsify or influence a device's location data.

Win/Place/Show – A wager type in which the player wagers on a selected participant to finish in a specified position. A "win" wager requires the participant to finish first; a "place" wager requires the participant to finish first or second; and a "show" wager requires the participant to finish first, second, or third, subject to the applicable rules of the wagering event and wager type.