State of Connecticut

Department of Consumer Protection

SPORTS WAGERING TECHNICAL SPECIFICATIONS

INTRODUCTION

The Connecticut Department of Consumer Protection ("DCP") has prepared this document to serve as a reference for technical specifications concerning Sports Wagering operations. This document is meant to serve as a framework based on existing technology and industry best practices to safeguard the interest of the consumer and ensure the integrity of the gaming process.

This technical standard has been adopted by the DCP to supplement the Online Gaming and Retail Sports Wagering regulations. In the event of any conflict between these technical specifications and the Regulations promulgated pursuant to Public Act 21-23, the stricter standard shall control.

1.1.0 Software Suppliers and Operators

The components of an Electronic Wagering Platform, although they may be constructed in a modular fashion, are designed to work seamlessly together. In addition, Electronic Wagering Platform 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 Electronic Wagering Platform submitted by a software supplier in the absence of the final configuration chosen by the operator; however, the configuration that will be utilized in the production environment shall be communicated to the independent test laboratory to facilitate creating a functionally equivalent test environment. An up to date copy of the same and summary network architecture shall be provided to the DCP after certification by approved gaming laboratory.

1.1.2 System Clock

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

a) Time stamping of all transactions and games;
b) Time stamping of significant events; and
c) Reference clock for reporting.
d) All reference to time will use a common trusted established time source to synchronize all components.

The Electronic Wagering Platform shall be equipped with a mechanism to ensure the time and dates between all components that comprise the system are synchronized and set correctly.

1.1.3 Control Program Self-Verification

The Electronic Wagering Platform shall be capable of verifying that all critical control program components contained on the system are authentic copies of the approved components of the platform, at least once every twenty-four hours and on demand using a method approved by the DCP. The critical control program authentication mechanism shall:

a) Employ a cryptographic hash algorithm which produces a message digest of at least 256 bits. Other test methodologies shall be reviewed on a case-by-case basis;

b) Include all critical control program components which may affect gaming operations, including but not limited to executables, libraries, gaming or system configurations, operating system files, components that control required system reporting, and database elements that affect; and

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

d) System should self-verify that OS is up to date on all critical patches.

1.1.4 Control Program Independent Verification

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

1.1.5 Gaming Management

The Electronic Wagering Platform shall be able to disable the following on demand:

a) All wagering activity.
b) Individual events.
c) Individual markets.
d) Individual Wagering Devices (if applicable); and
e) Individual patron logins (if applicable).

2.0.0 Registration and Verification

There shall be a method to collect patron information prior to the registration of a patron account. Where patron account registration and verification are supported by the Electronic Wagering Platform either directly by the system or in conjunction with a third-party service provider's software, the following requirements shall be met:

a) Only patrons of the legal wagering age for the jurisdiction may register for a patron account. Any person that submits a birth date that indicates they are underage shall be denied the ability to register for a patron account.

b) Identity verification shall be undertaken before a patron is allowed to place a wager. Third-party service providers may be used for identity verification as allowed by the DCP.

i. Identity verification shall authenticate the legal name, physical address and age of the individual at a minimum as required by the DCP.

ii. Identity verification shall also confirm that the patron is not on any exclusion lists held by the operator or the DCP or prohibited from establishing or maintaining an account for any other reason.

iii. Details of identity verification shall be kept in a secure manner. c) The patron account can only become active once age and identity verification are successfully completed, the patron is determined to not be on any exclusion lists or prohibited from establishing or maintaining an account for any other reason, the patron has acknowledged the necessary privacy policies and terms and conditions, and the patron account registration is complete.

d) A patron shall only be permitted to have one active patron account at a time.

e) The platform shall allow the ability to update passwords, registration information and the account used for financial transactions for each patron. A multi-factor authentication process shall be employed for these purposes.

2.1.0. Patron Access

A patron accesses their patron account using a username (or similar) and a password or a secure alternative means for the patron to perform authentication to log in to the Electronic Wagering Platform. Authentication methods are subject to the discretion of the DCP as necessary. The requirement does not prohibit the option for more than one method of authentication being available for a patron to access their account.

a) If the platform does not recognize the username and/or password when entered, an explanatory message shall be displayed to the patron which prompts the patron to re-enter the information.

b) Where a patron has forgotten their username and/or password, a multi-factor authentication process shall be employed for the retrieval of the username/resetting of the password.

c) Current account balance information and transaction options shall be available to the patron once authenticated.

d) The platform shall support a mechanism that allows for an account to be locked in the event that suspicious activity is detected (e.g., too many failed attempts for login). A multi-factor authentication process shall be employed for the account to be unlocked.

2.1.2 Patron Inactivity

For patron accounts accessed remotely for wagering or account management, after 15 minutes of inactivity on that device, the patron shall be required to re-authenticate to access their patron account.

a) No further wagering or financial transactions on that device are permitted until the patron has been re-authenticated.

b) A simpler means may be offered for a patron to re-authenticate on that device, such as operating system-level authentication (e.g., biometrics) or a Personal Identification Number (PIN). Each means for re-authentication will be evaluated on a case-by-case basis by the independent test laboratory.

i. This functionality may be disabled based on preference of the patron and/or DCP.

ii. Once every 30 days, or a period specified by the DCP, the patron will be required to provide full authentication on that device.

2.1.3. Limitations and Exclusions

The Electronic Wagering Platform shall be able to correctly implement any limitations and/or exclusions put in place by the patron and/or operator as required by the DCP:

a) Where the system provides the ability to directly manage limitations and/or exclusions, the applicable requirements within the “Limitations” and “Exclusions” sections of this document shall be evaluated;
b) The self-imposed limitations set by a patron shall not override more restrictive operator-imposed limitations. The more restrictive limitations shall take priority; and
c) Limitations shall not be compromised by internal status events, such as self-imposed exclusion orders and revocations.

2.1.4. Patron Funds Maintenance

Where financial transactions can be performed automatically by the Electronic Wagering Platform the following requirements shall be met:

a) The system shall provide confirmation/denial of every financial transaction initiated.
b) A deposit into a patron account may be made via a credit card transaction or other methods which can produce a sufficient audit trail.
c) Funds shall not be available for wagering until they are received from the issuer or the issuer provides an authorization number indicating that the funds are authorized. The authorization number is to be maintained in an audit log.
d) Payments from an account are to be paid (including funds transfer) directly to an account with a financial institution in the name of the patron or made payable to the patron and forwarded to the patron’s address using a secure delivery service or through another method that is not prohibited by the DCP. The name and address are to be the same as held in patron registration details.
e) If a patron initiates a patron account transaction and that transaction would exceed limits put in place by the operator and/or DCP, this transaction may only be processed provided that the patron is clearly notified that they have withdrawn or deposited less than requested.
f) It shall not be possible to transfer funds between two patron accounts.

2.1.5 Transaction Log or Account Statement

The Electronic Wagering Platform shall be able to provide a transaction log or account statement history to a patron upon request. The information provided shall include sufficient information to allow the patron to reconcile the statement or log against their own financial records. Information to be provided shall include at a minimum, details on the following types of transactions:

a) Financial Transactions (time stamped with a unique transaction ID):
    i. Deposits to the patron account;
    ii. Withdrawals from the patron account;
    iii. Promotional or bonus credits added to/removed from the patron account (outside of credits won in wagering);
    iv. Manual adjustments or modifications to the patron account (e.g., due to refunds);
b) Wagering Transactions:
    i. Unique identification number of the wager;
    ii. The date and time the wager was placed;
    iii. The date and time the event started and ended or is expected to occur for future events (if known);
    iv. The date and time the results were confirmed (blank until confirmed);
    v. Any patron choices involved in the wager, including market and line postings, wager selection, and any special condition(s) applying to the wager; \
    vi. The results of the wager (blank until confirmed);

vii. Total amount wagered, including any promotional/bonus credits (if applicable);
viii.Total amount won, including any promotional/bonus credits (if applicable);
ix. Commission or fees collected (if applicable); and
x. The date and time the winning wager was paid to the patron.

2.2.1 Patron Loyalty Programs

Patron loyalty programs are any programs that provide incentives for patrons, typically based on the volume of play or revenue received from a patron. If patron loyalty programs are supported by the Electronic Wagering Platform, the following principles shall apply:

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

3.0.0 General Statement

Electronic Wagering Platform which support the issuance and/or redemption of wagering instruments (vouchers and coupons) shall meet the applicable requirements established within the “Machine Vouchers” section of the GLI-11 Standards for Gaming Devices and the “Validation System Requirements” of the GLI-13 Standards for On-Line Monitoring and Control Systems (MCS) and Validation Systems and other applicable jurisdictional requirements observed by the DCP.

3.0.1 General Statement

The requirements within this section shall apply when the Electronic Wagering Platform supports remote wagering. NOTE: The operator or third-party service provider maintaining these components, services and/or applications shall meet the auditing procedures indicated in the “Location Service Provider” section of this document.

3.0.2 Location Fraud Prevention

The Electronic Wagering Platform shall incorporate a mechanism to detect the use of remote desktop software, rootkits, virtualization, and/or any other programs identified as having the ability to circumvent location detection. This shall follow best practice security measures to, at a minimum, address the following:

a) Detect and block location data fraud (e.g., fake location apps, virtual machines, remote desktop programs, etc.) prior to completing each wager;
b) Examine the IP address upon each Patron Device connection to a network to ensure a known Virtual Private Network (VPN) or proxy service is not in use;
c) Detect and block devices which indicate system-level tampering (e.g., rooting, jailbreaking, etc.);
d) Stop "Man-In-The-Middle" attacks or similar hacking techniques and prevent code manipulation;
e) Utilize detection and blocking mechanisms verifiable to an application level; and

f) Monitor and prevent wagers placed by a single patron account from geographically inconsistent locations (e.g., wager placement locations were identified that would be impossible to travel between in the time reported).

3.0.3 Location Detection for Remote Wagering on a WLAN

Where remote wagering occurs over a Wireless Local Area Network (WLAN), the Electronic Wagering Platform shall incorporate at minimum, one of the following methods or similar functionality that can track the locations of all patrons connected to the WLAN:

a) A location detection service or application in which each patron shall pass a location check prior to completing each wager. This service or application shall meet the requirements specified in the next section for "Location Detection for Remote Wagering Over the Internet"; or
b) A location detection component that detects in real-time when any patrons are no longer in the permitted area and prevent further wagers from being placed. This can be accomplished with the use of specific IT hardware such as directional antennas, Bluetooth sensors or other methods to be evaluated on a case-by-case basis by the approved independent test laboratory.

3.0.4 Location Detection for Remote Wagering Over the Internet

Where remote wagering occurs over the internet, the Electronic Wagering Platform shall incorporate a location detection service or application to reasonably detect and dynamically monitor the location of a patron attempting to place a wager; and to monitor and enable the blocking of unauthorized attempts to place a wager.

a) Each patron shall pass a location check prior to completing the first wager after logging in on a specific Patron Device. Subsequent location checks on that device shall occur prior to completing wagers after a period of 30 minutes since the previous location check, or as otherwise specified by the DCP:
    i. If the location check indicates the patron is outside the permitted boundary or cannot successfully locate the patron, the wager shall be rejected, and the patron shall be notified of this.
    ii. An entry shall be recorded in a time stamped log any time a location violation is detected, including the unique patron ID and the detected location.
b) A geolocation method shall be used to provide a patron's physical location and an associated confidence radius. The confidence radius shall be entirely located within the permitted boundary.
c) Accurate location data sources (Wi-Fi, GSM, GPS, etc.) shall be utilized by the geolocation method to confirm the patron's location. If a Patron Device's only available location data source is an IP Address, the location data of a mobile device registered to the patron account may be used as a supporting location data source under the following conditions:
    i. The Patron Device (where the wager is being placed) and the mobile device shall be determined to be near one another.
    ii. If allowed by the DCP, carrier-based location data of a mobile device may be used if no other location data sources other than IP Addresses are available.

d) The geolocation method shall possess the ability to control whether the accuracy radius of the location data source is permitted to overlap or exceed defined buffer zones or the permitted boundary; and

e) To mitigate and account for discrepancies between mapping sources and variances in geospatial data, boundary polygons based on audited maps approved by the DCP as well as overlay location data onto these boundary polygons shall be utilized.

3.0.5 Data Retention and Time Stamping

The Electronic Wagering Platform shall be capable of maintaining and backing up all recorded data as discussed within this section:

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

3.0.6 Wager Record Information

For each individual wager placed by the patron, the information to be maintained and backed up by the Electronic Wagering Platform shall include:

a) The date and time the wager was placed;
b) Any patron choices involved in the wager:
    i. Market and line postings (e.g., money line bet, point spreads, over/under amounts, win/place/show);
    ii. Wager selection (e.g., athlete or team name and number);
    iii. Any special condition(s) applying to the wager;
c) The results of the wager (blank until confirmed);
d) Total amount wagered, including any promotional/bonus credits (if applicable);
e) Total amount won, including any promotional/bonus credits (if applicable);
f) Commission or fees collected (if applicable);
g) The date and time the winning wager was paid to the patron;
h) Unique identification number of the wager;
i) User identification or unique Wagering Device ID which issued the wager record (if applicable);
j) Relevant location information;
k) Event and market identifiers;
l) Current wager status (active, cancelled, unredeemed, pending, void, invalid, redemption in progress, redeemed, etc.);
m) Unique patron ID, for wagers conducted using a patron account;
n) Redemption period (if applicable); and
o) Open text field for attendant input of patron description or picture file (if applicable);

3.0.7 Market Information

For each individual market available for wagering, the information to be maintained and backed up by the Electronic Wagering Platform shall include:

a) The date and time the wagering period started and ended;
b) The date and time the event started and ended or is expected to occur for future events (if known);
c) The date and time the results were confirmed (blank until confirmed);
d) Total amount of wagers collected, including any promotional/bonus credits (if applicable);
e) The line postings that were available throughout the duration of a market (time stamped) and the confirmed result (win/loss/push);

f) Total amount of winnings paid to patrons, including any promotional/bonus credits (if applicable);
g) Total amount of wagers voided or cancelled, including any promotional/bonus credits (if applicable);
h) Commission or fees collected (if applicable);
i) Event status (in progress, complete, confirmed, etc.); and
j) Event and market identifiers.

3.0.8 Contest/Tournament Information

For Electronic Wagering Platforms which support contests/tournaments, the information to be maintained and backed up by the Electronic Wagering Platform shall include for each contest/tournament:

a) Name of the contest/tournament;
b) The date and time the contest/tournament occurred or will occur (if known);
c) Unique patron ID and name of each registered patron, amount of entry fee paid, and the date paid;
d) Unique patron ID and name of each winning patron, amount paid, and the date paid;
e) Total amount of entry fees collected, including any promotional/bonus credits (if applicable);
f) Total amount of winnings paid to patrons, including any promotional/bonus credits (if applicable);
g) Commission or fees collected (if applicable); and delineated by state/jurisdiction
h) Contest/tournament status (in progress, complete, etc.).

3.0.9 Patron Account Information

For Electronic Wagering Platforms which support patron account management, the information to be maintained and backed up by the Electronic Wagering Platform shall include for each patron account:

a) Unique patron ID and patron name;
b) Patron data (including verification method);
c) The date of patron agreement to the operator's terms and conditions and privacy policy;
d) Account details and current balance;
e) Open text field for attendant input of patron description or picture file (if applicable);
f) Previous accounts, if any, and reason for de-activation;
g) The date and method from which the account was registered (e.g., remote vs. on-site);
h) The date and time of last log in;
    i. Exclusions/limitations information as required by the DCP:
    i. The date and time of the request (if applicable);
    ii. Description and reason of exclusion/limitation;
    iii. Type of exclusion/restriction (e.g., operator-imposed exclusion, self-imposed limitation);
    iv. The date exclusion/limitation commenced;
    v. The date exclusion/limitation ended (if applicable);
j) Financial Transaction information:
    i. Type of transaction (e.g., deposit, withdrawal, adjustment);
    ii. The date and time of the transaction;
    iii. Unique transaction ID;

iv. Amount of transaction;
v. Total account balance before/after transaction;
vi. Total amount of fees paid for transaction (if applicable);
vii. User identification or unique Wagering Device ID which handled the transaction (if applicable);
viii. Transaction status (pending, complete, etc.);
ix. Method of deposit/withdrawal (e.g., cash, debit or credit card, personal check, cashier's check, wire transfer, money order);
x. Deposit authorization number; and
xi. Relevant location information.

3.1.0 Promotion/Bonus Information

For Electronic Wagering Platforms which support promotions and/or bonuses that are redeemable for cash, wagering credits, or merchandise, the information to be maintained and backed up by the Electronic Wagering Platform shall include for each promotion/bonus:

a) The date and time the promotion/bonus period started and ended or will end (if known);
b) Current balance for promotion/bonus;
c) Total amount of promotions/bonuses issued;
d) Total amount of promotions/bonuses redeemed;
e) Total amount of promotions/bonuses expired;
f) Total amount of promotion/bonus adjustments; and
g) Unique ID for the promotion/bonus.

3.1.1 Wagering Device Information

For each individual Self-Service Wagering Device or POS Wagering Device, the information to be maintained and backed up by the Electronic Wagering Platform shall include, as applicable:

a) Unique Wagering Device ID;
b) Wager record purchases;
c) Winning wager record redemptions, if supported;
d) Wager record voids and cancellations; and
e) User identification and session information, for POS Wagering Devices;

3.1.2 Significant Event Information

Significant event information to be maintained and backed up by the Electronic Wagering Platform shall include:

a) Failed login attempts;
b) Program error or authentication mismatch;
c) Significant periods of unavailability of any critical component of the system;
d) Large wins (single and aggregate over defined time period) in excess of a value specified by the DCP, including wager record information;
e) Large wagers (single and aggregate over defined time period) in excess of a value specified by the DCP, including wager record information;
f) System voids, overrides, and corrections;
g) Changes to live data files occurring outside of normal program and operating system execution;

h) Changes that are made to the download data library, including the addition, changing or deletion of software, where supported;
i) Changes to operating system, database, network, and application policies and parameters;
j) Changes to date/time on master time server;
k) Changes to previously established criteria for an event or market (not including line posting changes for active markets);
l) Changes to the results of an event or market;
m) Changes to promotion and/or bonus parameters;
n) Patron Account Management:
    i. Adjustments to a patron account balance;
    ii. Changes made to patron data and sensitive information recorded in a patron account;
    iii. Deactivation of a patron account;
    iv. Large financial transactions (single and aggregate over defined time period) in excess of a value specified by the DCP, including transaction information;
o) Irrecoverable loss of sensitive information;
p) Any other activity requiring user intervention and occurring outside of the normal scope of system operation; and
q) Other significant or unusual events as deemed applicable by the DCP.

3.1.3 User Access Information

For each user account, the information to be maintained and backed up by the Electronic Wagering Platform shall include:

a) Employee name and title or position;
b) User identification;
c) Full list and description of functions that each group or user account may execute;
d) The date and time the account was created;
e) The date and time of last log in;
f) The date and time of last password change;
g) The date and time the account was disabled/deactivated; and
h) Group membership of user account (if applicable).

3.1.4 General Reporting Requirements

The Electronic Wagering Platform shall be capable of generating the information needed to compile reports as required by the DCP. In addition to meeting the requirements in the section above for “Data Retention and Time Stamping”, the following requirements shall apply for required reports:

a) The system shall be able to provide the reporting information on demand and for intervals required by the DCP including, but not limited to, daily, month-to-date (MTD), year-to-date (YTD), and life-to-date (LTD).
b) Each required report shall contain:
    i. The operator, the selected interval and the date/time the report was generated; and
    ii. An indication of “No Activity” or similar message if no information appears for the period specified.

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

3.1.5 Operator Revenue Reports

The Electronic Wagering Platform shall be able to provide the following information needed to compile one or more reports on operator revenue for each event as a whole and for each individual market within that event which may be used for operator taxation information:

a) The date and time each event started and ended;
b) Total amount of wagers collected;
c) Total amount of winnings paid to patrons;
d) Total amount of wagers voided or cancelled;
e) Commission and fees collected (if applicable);
f) Event and market identifiers; and
g) Event status (in progress, complete, confirmed, etc.).

3.1.6 Operator Liability Reports

The Electronic Wagering Platform shall be able to provide the following information needed to compile one or more reports on operator liability:

a) Total amount held by the operator for the patron accounts (if applicable);
b) Total amount of wagers placed on future events; and
c) Total amount of winnings owed but unpaid by the operator on winning wagers.

3.1.7 Future Events Reports

The Electronic Wagering Platform shall be able to provide the following information needed to compile one or more reports on future events for the gaming day:

a) Wagers placed prior to the gaming day for future events (total and by wager);
b) Wagers placed on the gaming day for future events (total and by wager);
c) Wagers placed prior to the gaming day for events occurring on that same day (total and by wager);
d) Wagers placed on the gaming day for events occurring on that same day (total and by wager);
e) Wagers voided or cancelled on the gaming day (total and by wager); and
f) Event and market identifiers.

3.1.8 Significant Events and Alterations Reports

The Electronic Wagering Platform shall be able to provide the following information needed to compile one or more reports for each significant event or alteration as applicable:

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

3.1.9 General Statement

A wager may be placed using one of the following types of Wagering Devices as allowed by the DCP. Any other types of Wagering Devices will be reviewed on a case-by-case basis, as allowed by the DCP.

a) Point-of-Sale (POS) Wagering Device: An attendant station that at a minimum will be used by an attendant for the execution or formalization of wagers placed on behalf of a patron.
b) Self-Service Wagering Device: A kiosk that at a minimum will be used for the execution or formalization of wagers placed by a patron directly and, if supported, may be used for redemption of winning wager records.
c) Patron Device: A patron-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 patron directly. Examples of a Patron Device include a personal computer, mobile phone, tablet, etc.

3.2.1 General Statement

Wagering Software is used to take part in wagering and financial transactions with the Electronic Wagering Platform which, based on design, is downloaded to or installed on the Wagering Device, run from the Electronic Wagering Platform which is accessed by the Wagering Device, or a combination of the two.

3.2.2 Software Identification

Wagering Software shall contain sufficient information to identify the software and its version.

3.2.3 Software Validation

For Wagering Software installed locally on the Wagering Device, it shall be possible to authenticate that all critical components contained in the software are valid each time the software is loaded for use, and where supported by the system, on demand as required by the DCP. Critical components may include, but are not limited to, wagering rules, elements that control the communications between the Wagering Device and the Electronic Wagering Platform, or other components that are needed to ensure proper operation of the software. In the event of a failed authentication (i.e., program mismatch or authentication failure), the software shall prevent wagering operations and display an appropriate error message.

NOTE: Program verification mechanisms will be evaluated on a case-by-case basis and approved by the DCP and the independent test laboratory based on industry-standard security practices.

3.2.4 User Interface Requirements

The user interface is defined as an interface application or program through which the user views and/or interacts with the Wagering Software. The user interface shall meet the following requirements:

a) The functions of all buttons, touch or click points shall be clearly indicated within the area of the button, or touch/click point or within the help menu. There shall be no functionality available through any buttons or touch/click points on the user interface that are undocumented.
b) Any resizing or overlay of the user interface shall be mapped accurately to reflect the revised display and touch/click points.
c) User interface instructions, as well as information on the functions and services provided by the software, shall be clearly communicated to the user and shall not be misleading or inaccurate.

d) The display of the instructions and information shall be adapted to the user interface. For example, where a Wagering Device uses technologies with a smaller display screen, it is permissible to present an abridged version of the wagering rules accessible directly from within the wagering screen and make available the full/complete version of the wagering rules via another method, such as a secondary screen, help menu, or other interface that is easily identified on the visual wagering screen.

3.2.5 Simultaneous Inputs

Wagering Software shall not be adversely affected by the simultaneous or sequential activation of the various inputs and outputs which might, whether intentionally or not, cause malfunctions or invalid results.

3.2.6 Wager Record Printers

If the Wagering Device uses a printer to issue printed wager records to the patron, the printed wager record shall include information as indicated in "Wager Record" section of this document. It may be permissible for some of this information to be contained on the ticket stock itself.

3.2.7 Communications

Wagering Software shall be designed or programmed such that it may only communicate with authorized components through secure communications. If communication between the Electronic Wagering Platform and the Wagering Device is lost, the software shall prevent further wagering operations and display an appropriate error message. It is permissible for the software to detect this error when the device tries to communicate with the system.

3.3.1 General Statement

A patron places a wager at a Self-Service Wagering Device by using funds from their patron account or by using peripheral devices as authorized by the DCP. In addition to the requirements for "Wagering Software", the applicable requirements established within the GLI-20 Standards for Kiosks and other applicable jurisdictional requirements observed by the DCP shall be met for all proprietary components of the Self-Service Wagering Device.

3.4.1 General Statement

A patron places a wager at POS Wagering Device by using funds from their patron account or by providing payment for the wager(s) directly to the attendant. In addition to the requirements for "Wagering Software", the requirements established in this section shall be met for POS Wagering Devices.

3.4.2 Touch Screen Displays

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

3.4.3 Printing Wager Records

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

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

3.4.4 Wireless POS Wagering Devices

For wireless POS Wagering Devices, the applicable requirements for "Client-Server Interactions" of the next section shall also be met. Additionally, communication shall only occur between the wireless POS Wagering Device and the Electronic Wagering Platform via authorized access points within the venue.

3.5.1 General Statement

A patron may only place a wager on a Patron Device by using funds from their patron account (i.e. anonymous wagering transactions are prohibited). Depending on the implementation(s) authorized by the DCP, Patron Devices may be used on an in-venue Wireless Local Area Network (WLAN) or over the internet. In addition to the requirements for "Wagering Software", the requirements established in this section shall be met for Patron Devices.

3.5.2 Client-Server Interactions

The patron may obtain/download an application or software package containing the Wagering Software or access the software via a browser to take part in wagering and financial transactions with the Electronic Wagering Platform.

a) Patrons shall not be able to use the software to transfer data to one another, other than chat functions (e.g., text, voice, video, etc.) and approved files (e.g., user profile pictures, photos, etc.);
b) The software shall not automatically alter any device-specified firewall rules to open ports that are blocked by either a hardware or software firewall;
c) The software shall not access any ports (either automatically or by prompting the user to manually access) which are not necessary for the communication between the Patron Device and the server;
d) If the software includes additional non-wagering related functionality, this additional functionality shall not alter the software's integrity in any way;
e) The software shall not possess the ability to override the volume settings of the Patron Device; and
f) The software shall not be used to store sensitive information. It is recommended that auto complete, password caching, or other methods that will fill in the password field are disabled by default for the software.

3.5.3 Compatibility Verification

During any installation or initialization and prior to commencing wagering operations, the Wagering Software used in conjunction with the Electronic Wagering Platform shall detect any incompatibilities or resource limitations with the Patron Device that would prevent proper operation of the software (e.g., software version, minimum specifications not met, browser type, browser version, plug-in version, etc.). If any incompatibilities or resource limitations are detected the software shall prevent wagering operations and display an appropriate error message.

3.5.4 Software Content

Wagering Software shall not contain any malicious code or functionality deemed to be malicious in nature by the DCP. This includes, but is not limited to, unauthorized file extraction/transfers, unauthorized device modifications, unauthorized access to any locally stored personal information (e.g., contacts, calendar, etc.) and malware.

3.5.5 Cookies

Where cookies are used, patrons shall be informed of the cookie use upon Wagering Software installation or during patron registration. When cookies are required for wagering, wagering cannot occur if they are not accepted by the Patron Device. All cookies used shall contain no malicious code.

3.5.6 Information Access

The Wagering Software shall be able to display, either directly from the user interface or from a page accessible to the patron, the items specified in the following sections of this document. For Patron Devices which only allow wagers within a venue, it is acceptable to disclose to the patron the means of obtaining the information required by this section:

a) “Wagering Rules and Content”;
b) “Patron Protection Information”;
c) “Terms and Conditions”;
d) “Privacy Policy”;
e) “Wagering Displays and Information”; and
f) “Results Display”.

NOTE: It is accepted that the system will unavoidably be subject to a certain degree of synchronization delay for updates to this information as displayed on the software, and it is possible that information may only be updated at the patron’s next interaction with the software which causes the on-screen information to be refreshed.

4.1.1 General Statement

This chapter sets forth technical requirements for wagering operations, including, but not limited to rules for wager placement and results for markets within an event.

4.2.1 Posting of Wagering Rules

Comprehensive wagering rules shall be posted by an operator for the markets and event types currently offered. Where the Wagering Software includes these wagering rules directly, the software will be evaluated against the requirements within the “Wagering Rules” section of this document.

4.2.2 Dynamic Wagering Information

The following information shall be made available without the need for placing a wager. Within a venue this information may be displayed on a Wagering Device and/or an external display.

a) Information regarding the events and markets available for wagering;
b) Current odds/payouts and prices for available markets;
c) For types of markets where individual wagers are gathered into pools:
    i. Up-to-date odds/payouts information for simple market pools. For complex market pools, it is accepted that there may be reasonable limitations to the up-to-date accuracy of the pool estimates displayed to the patron;
    ii. Up-to-date values of total investments for all market pools; and
    iii. The dividends of any decided market.

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

4.2.3 Patron Resources/Features

Where allowed by the DCP, patron resources/features may be provided such as one that offers advice, hints, or suggestions to a patron, or a data stream that may be used to externally facilitate wager selection, if they conform to the following requirements:

a) The patron shall be made aware of each resource/feature that is available, the advantage it offers (if any), and the options that exist for selection.
b) The method for obtaining each resource/feature shall be disclosed to the patron. Any patron resources/features that are offered to the patron for purchase shall clearly disclose the cost.
c) The availability and functionality of patron resources/features shall remain consistent for all patrons.
d) For peer-to-peer wagering, the patron shall be provided with sufficient information to make an informed decision, prior to participation, as to whether to participate with patron(s) who may possess such resources/features.

4.3.1 General Statement

Wagers are placed in conjunction with a patron account or by funds provided to a Wagering Device or an attendant. Depending on the type of Wagering Device, wagers may be placed directly by the patron or on behalf of a patron by an attendant.

NOTE: Wagers placed using a Patron Device may only be placed in conjunction with a patron account.

4.3.2 Placement of a Wager

The following rules only apply to the placement of a paid wager directly by a patron on the Wagering Device:

a) The method of placing a wager shall be straightforward, with all selections (including their order, if relevant) identified. When the wager involves multiple events (e.g., parlays), such groupings shall be identified.
b) Patrons shall have the ability to select the market they want to place a wager on.
c) Wagers shall not be automatically placed on behalf of the patron without the patron's consent/authorization.
d) Patrons 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 DCP and opted in by the patron.
e) Situations shall be identified where the patron has placed a wager for which the associated odds/payouts or prices have changed, and unless the patron has opted in to auto-accept changes as permitted by the DCP, provide a notification to confirm the wager given the new values.
f) Clear indication shall be provided that a wager has been accepted or rejected (in full or in part). Each wager shall be acknowledged and clearly indicated separately so that there is no doubt as to which wagers have been accepted.
g) For wagers conducted using a patron account:
    i. The account balance shall be readily accessible.
    ii. A wager shall not be accepted that could cause the patron to have a negative balance.
    iii. The account balance is to be debited when the wager is accepted by the system.

4.3.3 Intentionally Deleted

4.3.4 Wager Record

Upon completion of a wagering transaction, the patron shall have access to a wager record which contains the following information:

a) The date and time the wager was placed;
b) The date and time the event is expected to occur (if known);
c) Any patron choices involved in the wager:
    i. Market and line postings (e.g., money line bet, point spreads, over/under amounts, win/place/show, etc.);
    ii. Wager selection (e.g., athlete or team name and number);
    iii. Any special condition(s) applying to the wager;
d) Total amount wagered, including any promotional/bonus credits (if applicable);
e) Unique identification number and/or barcode of the wager;
f) User identification or unique Wagering Device ID which issued the wager record (if applicable);
g) Venue Name/Site Identifier (for printed wager record, it is permissible for this information to be contained on the ticket stock itself); and
h) Redemption period (for printed wager records it is permissible for this information to be contained on the ticket stock itself).

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

4.3.5 Wagering Period Close

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

4.3.6 Play-For-Free Mode

Where allowed by the DCP, the Electronic Wagering Platform may support play-for-free mode, which allows a patron to participate in wagering without paying. Play-For-Free mode shall use the same odds/payouts as are available in any paid version and shall not mislead the patron about the odds/payouts available in the paid version.

4.4.1 Results Display

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

a) It shall be possible for a patron to obtain the results of their wagers on any decided market once the results have been confirmed.

b) Any change of results (e.g., due to statistics/line corrections) shall be made available.

4.4.2 Payment of Winnings

Once the results of the event are entered and confirmed, the patron may receive payment for their winning wagers. This does not preclude the ability for the patron to perform a redemption for an adjusted payout before event conclusion where offered and allowed by the DCP.

4.4.3 Winning Wager Record Redemption

The following requirements apply to the redemption of a winning wager at a Wagering Device, as allowed by the DCP. This section does not apply to winning wagers tied to a patron account which automatically updates the account balance.

a) The Electronic Wagering Platform shall process winning wager record redemption according to the secure communication protocol implemented.

b) No winnings are issued to the patron prior to confirmation of winning wager record validity.

c) The Electronic Wagering Platform shall have the ability to identify and provide a notification in the case of invalid or unredeemable wager records for the following conditions:

i. Wager record cannot be found on file;

ii. Wager record is not a winner;

iii. Winning wager record has already been paid; or

iv. Amount of winning wager record differs from amount on file (requirement can be met by display of winning wager amount for confirmation during the redemption process).

d) The Electronic Wagering Platform shall update the wager record status on the database during each phase of the redemption process accordingly. In other words, whenever the wager record status changes, the system shall update the database.

4.6.1 General Statement

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

a) The Electronic Wagering Platform is acting as the “host wagering system” receiving, for its own markets, wagers from one or more external “guest wagering systems”; or b) The Electronic Wagering Platform is acting as a “guest wagering system” passing wagers to an external “host wagering system,” for that system’s markets.

NOTE: The requirements of this section apply to the interoperability of the Electronic Wagering Platform with the external wagering system and are not a complete evaluation of the external wagering system itself. The external wagering system may independently be subject to evaluation by the independent test laboratory per DCP discretion.

4.6.2 Information

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

a) If the host wagering system provides pari-mutuel wagering for the guest wagering system, the Electronic Wagering Platform shall be able to:

i. When acting as the guest wagering system, receive the current dividends for active pools sent from the host wagering system.

ii. When acting as the host wagering system, pass the current dividends for active pools to all receiving guest wagering systems.

b) If the host wagering system provides fixed odds wagering for the guest wagering system where the odds/payouts and prices can be dynamically changed, the Electronic Wagering Platform shall be able to:

i. When acting as the guest wagering system, receive the current odds/payouts and prices sent from the host wagering system whenever any odds/payouts and prices are changed.

ii. When acting as the host wagering system, pass the current odds/payouts and prices to all receiving guest wagering systems whenever any odds/payouts and prices are changed.

c) Change of event status information shall be passed from the host wagering system to the guest wagering system whenever any change occurs, including:

i. Withdrawn/reinstated selections;

ii. Altered event starting time;

iii. Individual markets opened/closed;

iv. Results entered/modified;

v. Results confirmed; and

vi. Event cancelled.

4.6.3 Wagers

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

a) Wagers placed on the guest wagering system shall receive clear acknowledgment of acceptance, partial acceptance (including details), or rejection sent by the host wagering system.
b) If the cost of the wager is determined by the host wagering system, there shall be a positive confirmation sequence in place to enable the patron to accept the wager cost and the guest wagering system to determine that there are enough funds in the account balance to meet the wager cost prior to making an offer to the host wagering system.
c) Where wagers may be placed in bulk, the following requirements apply:

i. If the stream of wagers is interrupted for any reason, there shall be a means available to determine where in the stream that the interruption occurred.

ii. No wager in the stream may be greater than the account balance. If such a wager is attempted, the entire stream is to be halted.

d) The account balance shall be debited an amount equaling the offer and cost to the host wagering system. The funds shall remain as a pending transaction with details of the offer to the host wagering system logged. On receipt of acknowledgment from the host wagering system, the appropriate adjustments shall be made to the "pending" account and the account balance on the guest wagering system.
e) Cancellation requests from the guest wagering system shall receive clear acknowledgment of acceptance or rejection by the host wagering system. The patron is not to be credited by the guest wagering system until final confirmation is received from the host wagering system including the amount of the voided or cancelled wager.

4.6.4 Results

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

Appendix A: Operational Audit for Wagering Procedures and Practices

A.1 Introduction

A.1.1 General Statement

This appendix sets forth procedures and practices for wagering operations which will be reviewed in an operational audit as a part of the Electronic Wagering Platform evaluation, including, but not limited to establishing wagering rules, suspending events, handling various wagering and financial transactions, creating markets, settling wagers, closing markets, cancellations of events, voiding or cancelling wagers, patron account management, fundamental practices relevant to the limitation of risks, and any other objectives established by the DCP.

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 DCP within their rules, regulations, and Minimum Internal Control Standards (MICS).

A.2 Internal Control Procedures

A.2.1 Internal Control Procedures

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

A.2.2 Information Management

The operator's internal controls shall include the processes for maintaining the recorded information specified under the section entitled "Information to be Maintained" for a period of five years or as otherwise specified by the DCP.

A.2.3 Risk Management

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

a) Automated and manual risk management procedures;
b) Employee management, including access controls and segregation of duties;
c) Information regarding identifying and reporting fraud and suspicious conduct;
d) Controls ensuring regulatory compliance;
e) Description of Anti-Money Laundering (AML) compliance standards including procedures for detecting structuring to avoid reporting requirements;
f) Description of all software applications that comprise the Electronic Wagering Platform;
g) Description of all types of wagers available to be offered by the operator; Copyright 2019 Gaming
h) Description of the method to prevent past-post wagers from being placed;
i) Description of all integrated third-party service providers; and
j) Any other information required by the DCP.

A.2.4 Restricted Patrons

The operator's internal controls shall describe the method to prevent patrons from wagering on events in which they might have insider information, including, but not limited to the following examples, as required by the DCP:

a) Patrons identified as employees, subcontractors, directors, owners, and officers of an operator, as well as those within the same household, shall not place wagers on any event, except in private pools where their association with the operator is clearly disclosed.
b) Patrons identified as professional or collegiate athletes, team employees and owners, coaches, managers, handlers, athletic trainers, league officials and employees, referees, umpires, sports agents, and employees of a patron or referee union, as well as those within the same household,
shall not place wagers on any event in the sport in which they participate, or in which the athlete they represent participates.

A.3 Patron Account Controls

A.3.1 Registration and Verification

Where patron account registration is done manually by the operator, procedures shall be in place to

satisfy the requirements for “Registration and Verification” as indicated within this document.

A.3.2 Fraudulent Accounts

The operator must have a documented public policy for the treatment of patron 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 patron providing access to underage persons; and
c) The handling of deposits, wagers, and wins associated with a fraudulent account.

A.3.3 Terms and Conditions

A set of terms and conditions shall be available to the patron. During the registration process and when any terms and conditions are materially updated (i.e. beyond any grammatical or other minor changes), the patron shall agree to the terms and conditions. The terms and conditions shall:

a) State that only individuals legally permitted by their respective jurisdiction can participate in wagering;
b) Advise the patron to keep their authentication credentials (e.g., password and username) secure;
c) Disclose all processes for dealing with lost authentication credentials, forced password changes, password strength and other related items;
d) Specify the conditions under which an account is declared inactive and explain what actions will be undertaken on the account once this declaration is made; and
e) Clearly define what happens to the patron’s pending wagers placed prior to any self-imposed or operator-imposed exclusion, including the return of all wagers, or settling all wagers, as appropriate.

A.3.4 Privacy Policy

A privacy policy shall be available to the patron. During the registration process and when the privacy policy is materially updated (i.e. beyond any grammatical or other minor changes), the patron shall agree to the privacy policy. The privacy policy shall state

a) The patron data required to be collected;
b) The purpose for information collection;
c) The period in which the information is stored;
d) The conditions under which information may be disclosed; and
e) An affirmation that measures are in place to prevent the unauthorized or unnecessary disclosure of the information.

A.3.5 Patron Data Security

Any information obtained in respect to the patron account, including patron data, shall be done in compliance with the privacy policy and local privacy regulations and standards observed by the DCP. In addition:

a) Any patron data which is not subject to disclosure pursuant to the privacy policy shall be kept confidential, except where the release of that information is required by law.
b) There shall be procedures in place for the security and sharing of patron data, funds in a patron account and other sensitive information as required by the DCP, including, but not limited to:

i. The designation and identification of one or more employees having primary responsibility for the design, implementation and ongoing evaluation of such procedures and practices;
ii. The procedures to be used to determine the nature and scope of all information collected, the locations in which such information is stored, and the storage devices on which such information may be recorded for purposes of storage or transfer;
iii. The measures to be utilized to protect information from unauthorized access; and
iv. The procedures to be used in the event the operator determines that a breach of data security has occurred, including required notification to the DCP.

A.3.6 Financial Transactions

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

a) Where financial transactions cannot be performed automatically by the Electronic Wagering Platform, procedures shall be in place to satisfy the requirements for "Patron Funds Maintenance" as indicated within this document.
b) Positive patron identification or authentication shall be completed before the withdrawal of any funds can be made by the patron.
c) A patron's request for withdrawal of funds (i.e., deposited and cleared funds and wagers won) shall be completed by the operator within a reasonable amount of time, unless there is a pending unresolved patron complaint/dispute or investigation. Such investigation shall be documented by the operator and available for review by the DCP.
d) The operator shall have security or authorization procedures in place to ensure that only authorized adjustments can be made to patron accounts, and these changes are auditable.

A.3.7 Limitations

Patrons shall be provided with a method to impose limitations for wagering parameters including, but not limited to deposits and wagers as required by the DCP. In addition, there shall be a method for the operator to impose any limitations for wagering parameters as required by the DCP.

a) Once established by a patron and implemented by the operator, it shall only be possible to reduce the severity of self-imposed limitations upon 24 hours' notice, or as required by the regulatory body;
b) Patrons shall be notified in advance of any operator-imposed limits and their effective dates. Once updated, operator-imposed limits shall be consistent with what is disclosed to the patron; and
c) Upon receiving any self-imposed or operator-imposed limitation order, the operator shall ensure that all specified limits are correctly implemented immediately or at the point in time (e.g., next login, next day) clearly indicated to the patron.

A.3.8 Exclusions

Patrons shall be provided with a method to exclude themselves from wagering for a specified period or indefinitely, as required by the DCP. In addition, there shall be a method for the operator to exclude a patron from wagering as required by the DCP.

a) Patrons shall be given a notification containing exclusion status and general instructions for resolution where possible;

b) Immediately upon receiving the exclusion order, no new wagers or deposits are accepted from that patron, until the exclusion has been removed;

c) While excluded, the patron shall not be prevented from withdrawing any or all of their account balance, provided that the operator acknowledges that the funds have cleared, and that the reason(s) for exclusion would not prohibit a withdraw; and

d) All advertising or marketing material shall not specifically target patrons that have been excluded from play.

A.3.9 Inactive Accounts

A patron account is considered to be inactive under the conditions as specified in the terms and conditions. Procedures shall be in place to:

a) Protect inactive patron accounts that contain funds from unauthorized access, changes or removal; and

b) Deal with unclaimed funds from inactive patron accounts, including returning any remaining funds to the patron where possible.

A.4 General Operating Procedures

A.4.1 Operator Reserves

The operator shall have processes in place for maintaining and protecting adequate cash reserves, as determined by the DCP, including segregated accounts of funds held for patron accounts and operational funds such as those used to cover unclaimed winning wagers, potential winning wagers for the gaming day, etc.

A.4.2 Protection of Patron Funds

The operator shall have processes in place to ensure funds in an operator account are either to be held in trust for the patron in a special purpose segregated account that is maintained and controlled by a properly constituted corporate entity that is not the operator and whose governing board includes one or more corporate directors who are independent of the operator and of any corporation related to or controlled by the operator. In addition, the operator shall have procedures that are reasonably designed to:

a) Ensure that funds generated from wagering are safeguarded and accounted for;

b) Make clear that the funds in the segregated account do not belong to the operator and are not available to creditors other than the patron whose funds are being held; and

c) Prevent commingling of funds in the segregated account with other funds including, without limitation, funds of the operator.

A.4.3 Taxation

The operator shall have a process in place to identify all wins that are subject to taxation (single wins or aggregate wins over a defined period as required) and provide the necessary information in accordance with each DCP's taxation requirements.

NOTE: Amounts won that exceed any jurisdictional specified limit shall require the appropriate documentation to be completed before the winning patron is paid.

A.4.4 Complaint/Dispute Process

The operator shall provide a method for a patron to make a complaint/dispute, and to enable the patron to notify the DCP 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 DCP.

a) Patrons shall be able to log complaints/disputes on a 24/7 basis.
b) Records of all correspondence relating to a complaint/dispute shall be maintained for a period of five years or as otherwise specified by the DCP.
c) A documented process shall exist between the operator and the DCP on the complaint/dispute reporting and resolution process.

A.4.5 Patron Protection Information

Patron protection information shall be available to the patron. The patron protection information shall contain at a minimum:

a) Information about potential risks associated with excessive wagering, and where to get help for a gambling problem;
b) A statement that no underage persons are permitted to participate in wagering;
c) A list of the available patron protection measures that can be invoked by the patron, such as self-imposed exclusion, and information on how to invoke those measures;
d) For patron accounts, mechanisms in place which can be used to detect unauthorized use of their account, such as reviewing credit card statements against known deposits;
e) Contact information or other means for reporting a complaint/dispute; and
f) Contact information for the DCP and/or a link to their website.

A.5 Wagering Rules and Content

A.5.1 Wagering Rules

Wagering rules refers to any written, graphical, and auditory information provided to the public regarding event wagering operations. The operator shall adopt, and adhere to comprehensive wagering rules which shall be approved by the DCP:

a) Wagering rules shall be complete, unambiguous, and not misleading or unfair to the patron.
b) Wagering rules that are presented aurally (via sound or voice) shall also be displayed in written form.
c) Wagering rules shall be rendered in a color that contrasts with the background color to ensure that all information is clearly visible/readable.
d) The operator shall keep a log of any changes to the wagering rules relating to placing wagers.
e) Where wagering rules are altered for events or markets being offered, all rule changes shall be time and date stamped showing the rule applicable in each period. If multiple rules apply to an event or market, the operator shall apply the rules that were in place when the wager was

accepted.

A.5.2 Wagering Rules Content

The following information shall be made available to the patron. For wagers placed within a venue, it is acceptable for this information to be displayed by the Wagering Device directly or by external signage, forms, or brochures available:

a) The methods of funding a wager or patron account, including a clear and concise explanation of all fees (if applicable);
b) As allowed by the DCP, any prizes that are offered in the form of merchandise, annuities, lump sum payments, or payment plans instead of cash payouts for each market that is offering such a prize;
c) The procedures by which any unrecoverable malfunctions of hardware/software are addressed including if this process results in the voiding or cancelling of any wagers; and
d) The procedures to deal with interruptions caused by the discontinuity of data flow from the network server during an event.
e) Rules of participation, including all wagering eligibility and scoring criteria, available events and markets, types of wagers accepted, line postings, all advertised awards, and the effect of schedule changes;
f) Payout information, including possible winning positions, rankings, and achievements, along with their corresponding payouts, for any available wager option;
g) Any restrictive features of wagering, such as wager amounts or maximum win values;
h) A description on restricted patrons, including any applicable limitations on wagering for them (e.g. athletes shall not wager on their sport);
i) The procedures for handling incorrectly posted events, markets, odds/payouts, prices, wagers, or results;
j) A wager cancellation policy which shall cater for wagers with multiple events (e.g., parlays) and indicate any prohibitions of voiding or cancelling wagers (e.g., after a fixed time period);
k) Whether the odds/payouts are locked-in at the time of the wager, or if the odds/payouts may change dynamically prior to the commencement of the event and the method of noticing changes to the odds/payouts;
l) For types of wagers where the odds/payouts are fixed at the time the wager is placed, any situations where the odds/payouts may be adjusted such as atypical winning outcomes (e.g., dead heats), cancelled legs of wagers with multiple events (e.g., parlays), and prorating;
m) For types of wagers where individual wagers are gathered into pools, the rules for dividend calculation including the prevailing formula for pool allocations and the stipulations of the event being wagered upon as approved by the DCP;
n) For in-play wagering, due to varying communication speeds or broadcast transmission latencies:

i. Updates of the displayed information may put a patron at a disadvantage to others who may have more up-to-date information; and
ii. There may be delays incorporated in the registered time of an in-play wager to prevent pastpost wagers and cancellations.

o) A statement that the operator reserves the right to:

i. Refuse any wager or part of a wager or reject or limit selections prior to the acceptance of a wager for reasons indicated to the patron in these rules;
ii. Accept a wager at other than posted terms; and
iii. Close wagering periods at their discretion;

p) If prizes are to be paid for combinations involving participants other than solely the first-place finisher (e.g., in an Olympic competition), the order of the participants that can be involved with these prizes (e.g., result 8-4-7);
q) The rules for any exotic wagering options (e.g., perfecta, trifecta, quinella, etc.) and the expected payouts;
r) What is to occur when an event or market is cancelled or withdrawn, including the handling of selections wagers with multiple events (e.g., parlays) where one or more of these legs are cancelled or withdrawn;
s) How a winning wager is determined and the handling of an award in any case where a tie is possible;
t) The payment of winning wagers, including the redemption period and the method for calculation. Where the calculation of payouts may involve rounding, information on how these circumstances are handled shall clearly explain:

i. Rounding up, down (truncation), true rounding; and
ii. Rounding to what level (e.g., 5 cents).

A.5.3 Promotions and/or Bonuses

Patrons shall be able to access information in the wagering rules pertaining to any available promotions and/or bonuses, including how the patron is notified when they have received a promotional award or bonus win and the terms of their withdrawal. This information shall be clear and unambiguous, especially where promotions or bonuses are limited to certain events, markets, or when other specific conditions apply.

A.5.4 Contests/Tournaments

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

a) Rules shall be made available to a patron for review prior to contest/tournament registration. The rules shall include at a minimum:

i. All conditions registered patrons shall meet to qualify for entry and advancement through, the contest/tournament;
ii. Specific information pertaining to any single contest/tournament, including the available prizes or awards and distribution of funds based on specific outcomes; and
iii. The name of the organization (or persons) that conducted the contest/tournament on behalf of, or in conjunction with, the operator (if applicable).

b) Procedures shall be in place to record the results of each contest/tournament and make publicly available for the registered patrons to review for a reasonable period of time. Subsequent to being posted publicly, the results of each contest/tournament shall be made available upon request. The results include the following:

i. Name of the contest/tournament;
ii. Date(s)/times(s) of the contest/tournament;
iii. Total number of entries;
iv. Amount of entry fees;
v. Total prize pool; and
vi. Amount paid for each winning category.

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

A.6 Wagering Procedures and Controls

A.6.1 Odds/Payouts and Prices

There shall be established procedures for setting and updating the odds/payouts and prices including publicly providing the current odds/payouts and prices, changing odds/payouts and prices as necessary to handle exceptions, and properly logging and periodically logging the odds/payouts and prices.

A.6.2 Statistics/Line Data

The operator shall ensure that any statistics/line data that is made available to the patron pertaining to an event uses a source allowed by the DCP and is kept reasonably accurate and updated. As required by the DCP, controls shall be implemented for the operator to:

a) Review the accuracy and timeliness of any statistics/line services; and

b) When an incident or error occurs that results in a loss of communication with statistics/line services, record the incident or error in a log along with the date and time of occurrence, its duration, nature, and a description of its impact on the system's performance. This information shall be maintained for a period of 90 days, or as otherwise specified by the DCP.

A.6.3 Suspending Markets or Events

There shall be established procedures for suspending markets or events (i.e. stop accepting wagers for that market or markets associated with that event). When wagering is suspended for an active event, an entry shall be made in an audit log that includes the date and time of suspension and its reason.

A.6.4 Wager Cancellations

Wagering transactions cannot be modified except to be voided or cancelled as provided for in the operator's published cancellation policy. A cancellation grace period may be offered to allow patrons to request a cancellation of wagers placed. The following requirements apply to wager cancellations:

a) Patron initiated cancellations may be authorized in accordance with the cancellation policy.

b) Operator initiated cancellations shall provide a reason for cancellation to a patron (e.g., past-post wager).

c) An operator shall not void or cancel any wager without the prior approval of the DCP.

A.6.5 Wagering

Documentation shall be in place to provide how the wagering period is controlled. This would include any cases where the wagering period is first opened, when it is closed, or any other time in between where a wager is unable to be placed (e.g., odds/payouts and prices are being updated).

A.6.6 Results

Before publicly announcing results and declaring winners, there shall be a policy for the confirmation of results based on qualified and approved sources, unless automated by an external feed. If an external feed is in use, there shall be procedures in place for cases where access to the external feed is unavailable. There shall also be a procedure in place to handle changes in results (e.g., due to statistics/line corrections).

A.6.7 Winning Wager Payment

In the event of a failure of the Electronic Wagering Platform's ability to pay winning wagers, the operator shall have controls detailing the method of paying these wagers.

A.6.8 Virtual Events

An operator who offers virtual event wagering shall maintain all information necessary to adequately reconstruct the virtual events, including the virtual event outcome and/or virtual participant actions, conducted within the past 90 days or as required by the DCP. This information may be recorded by the Electronic Wagering Platform or associated equipment, using some combination of text, logs, video, graphics, screen captures, or other means (e.g., "flight recorder" mechanism). Alternatively, procedures may be included to have the public display of the virtual event be recorded by the surveillance system.

A.7 Wagering Venue Specifications

A.7.1 Venue Verification Audit

The wagering venue will be required to meet the applicable aspects of the appropriate policy and/or procedure documents as determined by the operator in consultation with the DCP. To maintain the integrity of wagering operations, venues may be subject to an additional verification audit as required by the DCP. The following specifications apply to venues:

A.7.2 Wagering Equipment

The venue shall provide a secure location for the placement, operation, and usage of wagering equipment, including Wagering Devices, displays, and communications equipment. Security policies and procedures shall be in place and reviewed periodically to ensure that risks are identified, mitigated and underwritten by contingency plans. In addition:

a) Wagering equipment shall be installed according to a defined plan and records of all installed wagering equipment shall be maintained.

b) Wagering equipment shall be sited or protected to reduce the risks from

i. Environmental threats and hazards;

ii. Opportunities for unauthorized access;

iii. Power failures; and

iv. Other disruptions caused by failures in supporting utilities.

c) Access to the wagering equipment by an employee shall be controlled by a secure logon procedure or other secure process approved by the DCP to ensure that only authorized employees are allowed access. It shall not be possible to modify the configuration settings of the wagering equipment without an authorized secure process.

d) A user session, where supported by wagering equipment, is initiated by the employee logging in to their user account using their secure username and password or an alternative means for the employee to provide identification information as allowed by the DCP.

i. All available options presented to the employee shall be tied to their user account.

ii. If the wagering equipment does not receive input from the employee within 5 minutes, or a period specified by the DCP, the user session shall time out or lock up, requiring the employee to re-establish their login in order to continue.

e) To ensure its continued availability and integrity, wagering equipment shall be correctly maintained, inspected and serviced at regular intervals to ensure that it is free from defects or mechanisms that could interfere with its operation.

f) Prior to disposal or re-use, wagering equipment containing storage media shall be checked to ensure that any licensed software, patron account information, and other sensitive information has been removed or securely overwritten (i.e., not just deleted).

A.7.3 Wagering Operations

The following procedures shall be in place for wagering operations within the venue:

a) Procedures to enable a suitable response to any security issue within the venue.

b) Procedures to prevent any person from tampering with or interfering with the operation of any wagering or wagering equipment;

c) Procedures to describe the operations and the servicing of POS Wagering Devices and SelfService Wagering Devices, including the handling of error conditions and performing reconciliations;

d) Procedures to ensure accessibility requirements observed by the DCP are met for the installation of Self-Service Wagering Devices.

e) Procedures for wager transactions using a POS Wagering Device, including:

i. Accepting wagers from patrons only during the wager period;

ii. Notifying patrons if their wager attempt is rejected;

iii. Requiring the recording of patron data or patron account registration if their wager exceeds a value specified by the DCP;

iv. Providing notification of any odds/payouts or price changes which occur while attempting to process a wager;

v. Providing a patron access to a wager record once the wager is authorized;

f) Procedures for handling cancelled events and withdrawn selections for wagers with multiple events (e.g., parlays), including providing refunds to patrons who were not refunded automatically by the system (e.g., wagers placed anonymously); and

g) Procedures for redemption of winning wagers, including:

i. Scanning the barcode of a wager record (via a barcode reader or equivalent); or

ii. Manually inputting the wager identification number and performing a verification with the system.

A.7.4 Surveillance and Recording

The venue will be required to install, maintain, and operate a surveillance system that has the capability to monitor and record continuous unobstructed views of all wagering and financial transactions as well as any dynamic displays of wagering information. Procedures shall be in place to ensure that the recording:

a) Covers the defined wagering areas with sufficient detail to identify any discrepancies;

b) Is captured in such a way that precludes interference or deletion;
c) Can be reviewed by the operator and/or DCP in the event of a patron complaint/dispute; and
d) Is kept for at least 90 days or as required by the DCP.

A.8 Monitoring Procedures

A.8.1 Monitoring for Collusion and Fraud

The operator shall take measures designed to reduce the risk of collusion or fraud, including having procedures for:

a) Identifying and/or refusing to accept suspicious wagers which may indicate cheating, manipulation, interference with the regular conduct of an event, or violations of the integrity of any event on which wagers were made;
b) Reasonably detecting irregular patterns or series of wagers to prevent patron collusion or the unauthorized use of artificial patron software; and
c) Monitoring and detecting events and/or irregularities in volume or swings in odds/payouts and prices which could signal suspicious activities as well as all changes to odds/payouts and prices and/or suspensions throughout an event.

A.8.2 Anti-Money Laundering (AML) Monitoring

The operator shall have AML procedures and policies put in place, as required by the DCP, to ensure that:

a) Employees are trained in AML, and this training is kept up to date;
b) Patron accounts are monitored for opening and closing in short time frames and for deposits and withdrawals without associated wagering transactions; and
c) Aggregate transactions over a defined period may require further due diligence checks and may be reportable to the relevant organization if they exceed the threshold prescribed by the DCP.

A.8.3 Location Service Provider Monitoring

The operator, who offers remote wagering, or a third-party location service provider authorized by the DCP shall, where required by the DCP:

a) Have procedures to maintain a real-time data feed of all location checks and an up-to-date list of potential location fraud risks (e.g., fake location apps, virtual machines, remote desktop programs, etc.);
b) Offer an alert system to identify unauthorized or improper access;
c) Allow periodic audits to assess and measure its continued ability to detect and mitigate existing and emerging location fraud risks;
d) Ensure the location detection service or application used for location detection:
    i. Utilizes closed-source databases (IP, proxy, VPN, etc.) that are frequently updated and periodically tested for accuracy and reliability; and
    ii. Undergoes frequent updates to maintain cutting-edge data collection, device compatibility, and fraud prevention capabilities against location fraud risks.

Appendix B: Operational Audit for Technical Security Controls

B.1 Introduction

B.1.1 General Statement

This appendix sets forth technical security controls which will be reviewed in an operational audit as a part of the Electronic Wagering Platform evaluation, including, but not limited to, an information security system (ISS) assessment, review of the operational processes that are critical to compliance, penetration testing focused on the external and internal infrastructure as well as the applications transferring, storing and/or processing patron data and/or sensitive information, and any other objectives established by the DCP. The security controls outlined in this appendix apply to the following critical components of the system:

a) Components which record, store, process, share, transmit or retrieve sensitive information (e.g., validation numbers, PINs, patron data);
b) Components which generate, transmit, or process random numbers used to determine the outcome of virtual events (if applicable);
c) Components which store results or the current state of a patron's wager;
d) Points of entry to and exit from the above components (other systems which are able to communicate directly with core critical systems); and
e) Communication networks which transmit sensitive information.

NOTE: It is also recognized that additional technical security controls which are not specifically included within this standard will be relevant and required for an operational audit as determined by the DCP within their rules, regulations, and Minimum Internal Control Standards (MICS).

B.2 System Operation & Security

B.2.1 System Procedures

The operator shall be responsible for documenting and following the relevant Event Wagering System procedures. These procedures shall at least include the following as required by the DCP:

a) Procedures for monitoring the critical components and the transmission of data of the entire system, including communication, data packets, networks, as well as the components and data transmissions of any third-party services involved, with the objective of ensuring integrity, reliability and accessibility;
b) Procedures and security standards for the maintenance of all aspects of security of the system to ensure secure and reliable communications, including protection from hacking or tampering;
c) Procedures for defining, monitoring, documenting, and reporting, investigating, responding to, and resolving security incidents, including detected breaches and suspected or actual hacking or tampering with the system;
d) Procedure for monitoring and adjusting resource consumption and maintaining a log of the system performance, including a function to compile performance reports;
e) Procedures to investigate, document and resolve malfunctions, which address the following:
    i. Determination of the cause of the malfunction;
    ii. Review of relevant records, reports, logs, and surveillance records;
    iii. Repair or replacement of the critical component;
    iv. Verification of the integrity of the critical component before restoring it to operation;

v. Filing an incident report with the DCP and documenting the date, time and reason for the malfunction along with the date and time the system is restored; and
vi. Voiding or cancelling wagers and pays if a full recovery is not possible.

B.2.2 Physical Location of Servers

The Electronic Wagering Platform server(s) shall be housed in one or more secure location(s) which may be located locally, within a single venue, or may be remotely located outside of the venue as allowed by the DCP. In addition, secure location(s) shall:

a) Have sufficient protection against alteration, tampering or unauthorized access;
b) Be equipped with a surveillance system that shall meet the procedures put in place by the DCP;
c) Be protected by security perimeters and appropriate entry controls to ensure that access is restricted to only authorized personnel and that any attempts at physical access are recorded in a secure log; and
d) Be equipped with controls to provide physical protection against damage from fire, flood, hurricane, earthquake and other forms of natural or manmade disaster.

B.2.3 Logical Access Control

The Electronic Wagering Platform shall be logically secured against unauthorized access by authentication credentials allowed by the DCP, such as passwords, multi-factor authentication, digital certificates, PINs, biometrics, and other access methods (e.g., magnetic swipe, proximity cards, embedded chip cards).

a) Each user shall have their own individual authentication credential whose provision shall be controlled through a formal process.
b) Authentication credential records shall be maintained either manually or by systems that automatically record authentication changes and force authentication credential changes.
c) The storage of authentication credentials shall be secure. If any authentication credentials are hard coded on a component of the system, they shall be encrypted.
d) A fallback method for failed authentication (e.g., forgotten passwords) shall be at least as strong as the primary method.
e) Lost or compromised authentication credentials and authentication credentials of terminated users shall be deactivated, secured or destroyed as soon as reasonably possible.
f) The system shall have multiple security access levels to control and restrict different classes of access to the server, including viewing, changing or deleting critical files and directories. Procedures shall be in place to assign, review, modify, and remove access rights and privileges to each user, including:
    i. Allowing the administration of user accounts to provide an adequate separation of duties;
    ii. Limiting the users who have the requisite permissions to adjust critical system parameters;
    iii. The enforcement of adequate authentication credential parameters such as minimum length, and expiration intervals; and
g) Procedures shall be in place to identify and flag suspect accounts where authentication credentials may have been stolen.
h) Any logical access attempts to the system applications or operating systems shall be recorded in a secure log.

i) The use of utility programs which can override application or operating system controls shall be restricted and tightly controlled.

NOTE: Where passwords are used as an authentication credential, it is recommended that they are changed at least once every 90 days, are at least 8 characters in length and contain a combination of at least two of the following criteria: upper case letters, lower case letters, numeric and/or special characters.

B.2.4 User Authorization

The Electronic Wagering Platform shall implement the following user authorization requirements:

a) A secure and controlled mechanism shall be employed that can verify that the system component is being operated by an authorized user on demand and on a regular basis as required by the DCP.

b) The use of automated equipment identification to authenticate connections from specific locations and equipment shall be documented and shall be included in the review of access rights and privileges.

c) Any authorization information communicated by the system for identification purposes shall be obtained at the time of the request from the system and not be stored on the system component.

d) The system shall allow for system administrator notification and user lockout or audit trail entry, after a set number of unsuccessful authorization attempts.

B.2.5 Server Programming

The Electronic Wagering Platform shall be sufficiently secure to prevent any user-initiated programming capabilities on the server that may result in modifications to the database. However, it is acceptable for network or system administrators to perform authorized network infrastructure maintenance or application troubleshooting with sufficient access rights. The server shall also be protected from the unauthorized execution of mobile code.

B.2.6 Verification Procedures

There shall be procedures in place for verifying on demand that the critical control program components of the Electronic Wagering Platform in the production environment are identical to those approved by the DCP.

a) Signatures of the critical control program components shall be gathered from the production environment through a process to be approved by the DCP.

b) The process shall include one or more analytical steps to compare the current signatures of the critical control program components in the production environment with the signatures of the current approved versions of the critical control program components.

c) The output of the process shall be stored in an unalterable format, which detail the verification results for each critical control program authentication and:

i. Be recorded in a system log or report which shall be retained for a period of 90 days or as otherwise specified by the DCP;

ii. Be accessible by the DCP in a format which will permit analysis of the verification records by the DCP; and

iii. Comprise part of the system records which shall be recovered in the event of a disaster or equipment or software failure.

d) Any failure of verification of any component of the system shall require a notification of the authentication failure being communicated to the operator and DCP as required.

e) There shall be a process in place for responding to authentication failures, including determining
the cause of the failure and performing the associated corrections or reinstallations needed in a timely manner.

B.2.7 Electronic Document Retention System

Reports required by this standard and the DCP may be stored in an electronic document retention system provided that the system:

a) Is properly configured to maintain the original version along with all subsequent versions reflecting all changes to the report;

b) Maintains a unique signature for each version of the report, including the original;

c) Retains and reports a complete log of changes to all reports including who (user identification) performed the changes and when (date and time);

d) Provides a method of complete indexing for easily locating and identifying the report including at least the following (which may be input by the user):

i. Date and time report was generated;

ii. Application or system generating the report;

iii. Title and description of the report;

iv. User identification of who is generating the report; and

v. Any other information that may be useful in identifying the report and its purpose;

e) Is configured to limit access to modify or add reports to the system through logical security of specific user accounts;

f) Is configured to provide a complete audit trail of all administrative user account activity;

g) Is properly secured through use of logical security measures (user accounts with appropriate access, proper levels of event logging, and document the version control, etc.);

h) Is physically secured with all other critical components of the Electronic Wagering Platform; and

i) Is equipped to prevent disruption of report availability and loss of data through hardware and software redundancy best practices, and backup processes.

B.2.8 Asset Management

All assets housing, processing or communicating sensitive information, including those comprising the operating environment of the Electronic Wagering Platform and/or its components, shall be accounted for and have a nominated owner.

a) An inventory shall be drawn up and maintained of all assets holding controlled items.

b) A procedure shall exist for adding new assets and removing assets from service.

c) A policy shall be included on the acceptable use of assets associated with the system and its operating environment.

d) Each asset shall have a designated “owner” responsible for:

i. Ensuring that information and assets are appropriately classified in terms of their criticality, sensitivity, and value; and

ii. Defining and periodically reviewing access restrictions and classifications.

e) A procedure shall exist to ensure that recorded accountability for assets is compared with actual assets at intervals required by the DCP and appropriate action is taken with respect to discrepancies.
f) Copy protection to prevent unauthorized duplication or modification of software may be implemented provided that:

i. The method of copy protection is fully documented and provided to the independent test laboratory, to verify that the protection works as described; or
ii. The program or component involved in enforcing the copy protection can be individually verified by the methodology approved by the DCP.

B.3 Backup and Recovery

B.3.1 Data Security

The Electronic Wagering Platform shall provide a logical means for securing the patron data and wagering data, including accounting, reporting, significant event, or other sensitive information, against alteration, tampering, or unauthorized access.

a) Appropriate data handling methods shall be implemented, including validation of input and rejection of corrupt data.
b) The number of workstations where critical applications or associated databases may be accessed shall be limited.
c) Encryption or password protection or equivalent security shall be used for files and directories containing data. If encryption is not used, the operator shall restrict users from viewing the contents of such files and directories, which at a minimum shall provide for the segregation of system duties and responsibilities as well as the monitoring and recording of access by any person to such files and directories.
d) The normal operation of any equipment that holds data shall not have any options or mechanisms that may compromise the data.
e) No equipment may have a mechanism whereby an error will cause the data to automatically clear.
f) Any equipment that holds data in its memory shall not allow removal of the information unless it has first transferred that information to the database or other secured component(s) of the system.
g) Data shall be stored in areas of the server that are encrypted and secured from unauthorized access, both external and internal.
h) Production databases containing data shall reside on networks separated from the servers hosting any user interfaces.
i) Data shall be maintained at all times regardless of whether the server is being supplied with power.
j) Data shall be stored in such a way as to prevent the loss of the data when replacing parts or modules during normal maintenance.

B.3.2 Data Alteration

The alteration of any accounting, reporting or significant event data shall not be permitted without supervised access controls. In the event any data is changed, the following information shall be documented or logged:

a) Unique ID number for the alteration;

b) Data element altered;
c) Data element value prior to alteration;
d) Data element value after alteration;
e) Time and date of alteration; and
f) Personnel that performed alteration (user identification).

B.3.3 Backup Frequency

Backup scheme implementation shall occur at least once every day or as otherwise specified by the DCP, although all methods will be reviewed on a case-by-case basis.

B.3.4 Storage Medium Backup

Audit logs, system databases, and any other pertinent patron data and wagering data shall be stored using reasonable methods, including encryption in transit and storage. The Electronic Wagering Platform shall be designed to protect the integrity of this data in the event of a failure. Redundant copies of this data shall be kept on the system with open support for backups and restoration, so that no single failure of any portion of the system
would cause the loss or corruption of data.

a) The backup shall be contained on a non-volatile physical medium, or an equivalent architectural implementation, so that should the primary storage medium fail, the functions of the system and the process of auditing those functions can continue with no critical data loss.
b) Where the DCP allows for the use of cloud platforms, if the backup is stored in a cloud platform, another copy should be stored in a different non-cloud environment.
c) If hard disk drives are used as backup media, data integrity shall be assured in the event of a disk failure. Acceptable methods include, but are not limited to, multiple hard drives in an acceptable RAID configuration, or mirroring data over two or more hard drives.
d) Upon completion of the backup process, the backup media is immediately transferred to a location physically separate from the location housing the servers and data being backed up (for temporary and permanent storage).

i. The storage location is secured to prevent unauthorized access and provides adequate protection to prevent the permanent loss of any data.
ii. Backup data files and data recovery components shall be managed with at least the same level of security and access controls as the system.

NOTE: The distance between the two locations should be determined based on potential environmental threats and hazards, power failures, and other disruptions but should also consider the potential difficulty of data replication as well as being able to access the recovery site within a reasonable time (Recovery Time Objective).

B.3.5 System Failure

The Electronic Wagering Platform shall have sufficient redundancy and modularity so that if any single component or part of a component fails, the functions of the system and the process of auditing those functions can continue with no critical data loss. When two or more components are linked:

a) The process of all wagering operations between the components shall not be adversely affected by restart or recovery of either component (e.g., transactions are not to be lost or duplicated because of recovery of one component or the other); and

b) Upon restart or recovery, the components shall immediately synchronize the status of all transactions, data, and configurations with one another.

B.3.6 Accounting of Master Resets

The operator shall be able to identify and properly handle the situation where a master reset has occurred on any component which affects wagering operations.

B.3.7 Recovery Requirements

In the event of a catastrophic failure when the Electronic Wagering Platform cannot be restarted in any other way, it shall be possible to restore the system from the last backup point and fully recover. The contents of that backup shall contain the following critical information including, but not limited to:

a) The recorded information specified under the section entitled “Information to be Maintained”;
b) Specific site or venue information such as configuration, security accounts, etc.;
c) Current system encryption keys; and
d) Any other system parameters, modifications, reconfiguration (including participating sites or venues), additions, merges, deletions, adjustments and parameter changes.

B.3.8 Uninterruptible Power Supply (UPS)

All system components shall be provided with adequate primary power. Where the server is a standalone application, it shall have an Uninterruptible Power Supply (UPS) connected and shall have sufficient capacity to permit a graceful shut-down and that retains all patron data and wagering data during a power loss. It is acceptable that the system may be a component of a network that is supported by a network-wide UPS provided that the server is included as a device protected by the UPS. There shall be a surge protection system in use if not incorporated into the UPS itself.

B.3.9 Business Continuity and Disaster Recovery Plan

A business continuity and disaster recovery plan shall be in place to recover wagering operations if the Electronic Wagering Platform’s production environment is rendered inoperable. The business continuity and disaster recovery plan shall:

a) Address the method of storing patron data and wagering data to minimize loss. If asynchronous replication is used, the method for recovering data shall be described or the potential loss of data shall be documented;
b) Delineate the circumstances under which it will be invoked;
c) Address the establishment of a recovery site physically separated from the production site;
d) Contain recovery guides detailing the technical steps required to re-establish wagering functionality at the recovery site; and
e) Address the processes required to resume administrative operations of wagering activities after the activation of the recovered system for a range of scenarios appropriate for the operational context of the system.

B.4 Communications

B.4.1 General Statement

This section will discuss the various wired and wireless communication methods, including communications performed across the internet or a public or third-party network, as allowed by the DCP.

B.4.2 Connectivity

Only authorized devices shall be permitted to establish communications between any system components. The Electronic Wagering Platform shall provide a method to:

a) Enroll and un-enroll system components;
b) Enable and disable specific system components;
c) Ensure that only enrolled and enabled system components, including Wagering Devices, participate in wagering operations; and
d) Ensure that the default condition for components shall be un-enrolled and disabled.

B.4.3 Communication

Each component of the Electronic Wagering Platform shall function as indicated by a documented secure communication protocol.

a) All protocols shall use communication techniques that have proper error detection and recovery mechanisms, which are designed to prevent intrusion, interference, eavesdropping and tampering. Any alternative implementations will be reviewed on a case-by-case basis and approved by the DCP.
b) All data communications critical to wagering or patron account management shall employ encryption and authentication.
c) Communication on the secure network shall only be possible between approved system components that have been enrolled and authenticated as valid on the network. No unauthorized communications to components and/or access points shall be allowed.

B.4.4 Communications Over Internet/Public Networks

Communications between any system components, including Wagering Devices, which takes place over internet/public networks, shall be secure by a means approved by the DCP. Patron data, sensitive information, wagers, results, financial information, and patron transaction information shall always be encrypted over the internet/public network and protected from incomplete transmissions, misrouting, unauthorized message modification, disclosure, duplication or replay.

B.4.5 Wireless Local Area Network (WLAN) Communications

Wireless Local Area Network (WLAN) communications, as allowed by the DCP, shall adhere to the applicable jurisdictional requirements specified for wireless devices and network security. In the absence of specific jurisdictional standards, the “Wireless Device Requirements” and “Wireless Network Security Requirements” of industry best practices acceptable to the DCP, such as GLI-26.

NOTE: It is imperative for operators to review and update internal control policies and procedures to ensure the network is secure and threats and vulnerabilities are addressed accordingly. Periodic inspection and verification of the integrity of the WLAN is recommended.

B.4.6 Network Security Management

Networks shall be logically separated such that there should be no network traffic on a network link which cannot be serviced by hosts on that link. The following requirements apply:

a) All network management functions shall authenticate all users on the network and encrypt all network management communications.

b) The failure of any single item shall not result in a denial of service.

c) An Intrusion Detection System/Intrusion Prevention System (IDS/IPS) shall be installed on the network which can listen to both internal and external communications as well as detect or prevent:

i. Distributed Denial of Service (DDOS) attacks;

ii. Shellcode from traversing the network;

iii. Address Resolution Protocol (ARP) spoofing; and

iv. Other "Man-In-The-Middle" attack indicators and sever communications immediately if detected.

d) In addition to the requirements in (c), an IDS/IPS installed on a WLAN shall be able to:

i. Scan the network for any unauthorized or rogue access points or devices connected to any access point on the network at least quarterly or as defined by the DCP;

ii. Automatically disable any unauthorized or rogue devices connected to the system; and

iii. Maintain a history log of all wireless access for at least the previous 90 days or as otherwise specified by the DCP. This log shall contain complete and comprehensive information about all wireless devices involved and shall be able to be reconciled with all other networking devices within the site or venue.

e) Network Communication Equipment (NCE) shall meet the following requirements:

i. NCE shall be constructed in such a way as to be resistant to physical damage to the hardware or corruption of the contained firmware/software by normal usage.

ii. NCE shall be physically secured from unauthorized access.

iii. System communications via NCE shall be logically secured from unauthorized access.

iv. NCE with limited onboard storage shall, if the audit log becomes full, disable all communication or offload logs to a dedicated log server.

f) All network hubs, services and connection ports shall be secured to prevent unauthorized access to the network. Unused services and non-essential ports shall be either physically blocked or software disabled whenever possible.

g) In virtualized environments, redundant server instances shall not run under the same hypervisor.

h) Stateless protocols, such as UDP (User Datagram Protocol), shall not be used for sensitive information without stateful transport. Note that although HTTP (Hypertext Transport Protocol) is technically stateless, if it runs on TCP (Transmission Control Protocol) which is stateful, this is allowed.

i) All changes to network infrastructure (e.g., network communication equipment DCPconfiguration) shall be logged.

j) Virus scanners and/or detection programs shall be installed on all systems. These programs shall be updated regularly to scan for new strains of viruses.

B.5 Third-Party Service Providers

B.5.1 Third-Party Communications

Where communications with third-party service providers are implemented, such as patron loyalty programs, financial services (banks, payment processors, etc.), location service providers, cloud service providers, statistics/line services, and identity verification services, the following requirements apply:

a) The Electronic Wagering Platform shall be capable of securely communicating with third-party service providers using encryption and strong authentication.

b) All login events involving third-party service providers shall be recorded to an audit file.

c) Communication with third-party service providers shall not interfere or degrade normal Event Wagering System functions.

i. Third-party service provider data shall not affect patron communications.

ii. Connections to third-party service providers shall not use the sFame network infrastructure as patron connections.

iii. Wagering shall be disabled on all network connections except for the patron network;

iv. The system shall not route data packets from third-party service providers directly to the patron network and vice-versa

v. The system shall not act as IP routers between patron networks and third-party service providers.

d) All financial transactions shall be reconciled with financial institutions and payment processors daily or as otherwise specified by the DCP.

B.5.2 Third-Party Services

The security roles and responsibilities of third-party service providers shall be defined and documented as required by the DCP. The operator shall have policies and procedures for managing them and monitoring their adherence to relevant security requirements:

a) Agreements with third-party service providers involving accessing, processing, communicating or managing the system and/or its components, or adding products or services to the system and/or its components shall cover all relevant security requirements.

b) The services, reports and records provided by the third-party service providers shall be monitored and reviewed annually or as required by the DCP.

c) Changes to the provision of third-party service providers, including maintaining and improving existing security policies, procedures and controls, shall be managed, taking account of the criticality of systems and processes involved and re-assessment of risks.

d) The access rights of third-party service providers to the system and/or its components shall be removed upon termination of their contract or agreement or adjusted upon change.

B.6 Technical Controls

B.6.1 Domain Name Service (DNS) Requirements

The following requirements apply to the servers used to resolve Domain Name Service (DNS) queries used in association with the Electronic Wagering Platform.

a) The operator shall utilize a secure primary DNS server and a secure secondary DNS server which are logically and physically separate from one another.

b) The primary DNS server shall be physically located in a secure data center.

c) Logical and physical access to the DNS server(s) shall be restricted to authorized personnel.

d) Zone transfers to arbitrary hosts shall be disallowed.
e) A method to prevent cache poisoning, such as DNS Security Extensions (DNSSEC), is required.
f) Multi-factor authentication shall be in place.
g) Registry lock shall be in place, so any request to change DNS server(s) will need to be verified manually.

B.6.2 Cryptographic Controls

A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

a) Any patron data and/or sensitive information shall be encrypted if it traverses a network with a lower level of trust.
b) Data that is not required to be hidden but shall be authenticated shall use some form of message authentication technique.
c) Authentication shall use a security certificate from an approved organization.
d) The grade of encryption used shall be appropriate to the sensitivity of the data.
e) The use of encryption algorithms shall be reviewed periodically to verify that the current encryption algorithms are secure.
f) Changes to encryption algorithms to correct weaknesses shall be implemented as soon as practical. If no such changes are available, the algorithm shall be replaced.
g) Encryption keys shall be stored on a secure and redundant storage medium after being encrypted themselves through a different encryption method and/or by using a different encryption key.

B.6.3 Encryption Key Management

The management of encryption keys shall follow defined processes established by the operator and submitted to the DCP for review. These defined processes shall cover the following:

a) Obtaining or generating encryption keys and storing them;
b) Managing the expiry of encryption keys, where applicable;
c) Revoking encryption keys;
d) Securely changing the current encryption keyset; and
e) Recovering data encrypted with a revoked or expired encryption key for a defined period after the encryption key becomes invalid.

B.7 Remote Access and Firewalls

B.7.1 Remote Access Security

Remote access is defined as any access from outside the system or system network including any access from other networks within the same site or venue. Remote access shall only be allowed if authorized by the DCP and shall:

a) Be performed via a secured method;
b) Have the option to be disabled;
c) Accept only the remote connections permissible by the firewall application and system settings;

d) Be limited to only the application functions necessary for users to perform their job duties:

i. No unauthorized remote user administration functionality (adding users, changing permissions, etc.) is permitted; and

ii. Unauthorized access to the operating system or to any database other than information retrieval using existing functions is prohibited.

NOTE: Remote access security will be reviewed on a case-by-case basis, in conjunction with the implementation of the current technology and approval from the DCP.

B.7.2 Remote Access Procedures and Guest Accounts

A procedure for strictly controlled remote access shall be established. It is acknowledged that the supplier may, as needed, access the system and its associated components remotely for product and user support or updates/upgrades, as permitted by the DCP and the operator. This remote access shall use specific guest accounts which are:

a) Continuously monitored by the operator;

b) Disabled when not in use; and

c) Restricted through logical security controls to access only the necessary application(s) and/or database(s) for the product and user support or providing updates/upgrades.

B.7.3 Remote Access Activity Log

The remote access application shall maintain an activity log which updates automatically depicting all remote access information, to include:

a) Identification of user(s) who performed and/or authorized the remote access;

b) Remote IP Addresses, Port Numbers, Protocols, and where possible, MAC Addresses;

c) Time and date the connection was made and duration of connection; and

d) Activity while logged in, including the specific areas accessed and changes made.

B.7.4 Firewalls

All communications, including remote access, shall pass through at least one approved applicationlevel firewall. This includes connections to and from any non-system hosts used by the operator.

a) The firewall shall be located at the boundary of any two dissimilar security domains.

b) A device in the same broadcast domain as the system host shall not have a facility that allows an alternate network path to be established that bypasses the firewall.

c) Any alternate network path existing for redundancy purposes shall also pass through at least one application-level firewall.

d) Only firewall-related applications may reside on the firewall.

e) Only a limited number of user accounts may be present on the firewall (e.g., network or system administrators only).

f) The firewall shall reject all connections except those that have been specifically approved.

g) The firewall shall reject all connections from destinations which cannot reside on the network from which the message originated (e.g., RFC1918 addresses on the public side of an internet firewall).

h) The firewall shall only allow remote access over the most up to date encrypted protocols.

B.7.5 Firewall Audit Logs

The firewall application shall maintain an audit log and shall disable all communications and generate an error if the audit log becomes full. The audit log shall contain:

a) All changes to configuration of the firewall;

b) All successful and unsuccessful connection attempts through the firewall; and

c) The source and destination IP Addresses, Port Numbers, Protocols, and where possible, MAC Addresses.

NOTE: A configurable parameter 'unsuccessful connection attempts' may be utilized to deny further connection requests should the predefined threshold be exceeded. The system administrator shall also be notified.

B.7.6 Firewall Rules Review

If required by the DCP, the firewall rules shall be periodically reviewed to verify the operating condition of the firewall and the effectiveness of its security configuration and rule sets and shall be performed on all the perimeter firewalls and the internal firewalls.

B.8 Change Management

B.8.1 General Statement

A change management policy is selected by the DCP for handling updates to the Event Wagering System and its components based on the propensity for frequent system upgrades and chosen risk tolerance. For systems that require frequent updates, a risk-based change management program may be utilized to afford greater efficiency in deploying updates. Risk-based change management programs typically include a categorization of proposed changes based on regulatory impact and define associated certification procedures for each category. The independent licensed test laboratory will evaluate the system and future modifications in accordance with the change management policy selected by the DCP.

B.8.2 Program Change Control Procedures

Program change control procedures shall be adequate to ensure that only authorized versions of programs are implemented on the production environment. These change controls shall include:

a) An appropriate software version control or mechanism for all software components and source code;

b) Records kept of all new installations and/or modifications to the system, including:

- i. The date of the installation or modification;
- ii. Details of the reason or nature of the installation or change such as new software, server repair, significant configuration modifications;
- iii. A description of procedures required to bring the new or modified component into service (conversion or input of data, installation procedures, etc.);
- iv. The identity of the user(s) performing the installation or modification;

c) A strategy for reverting back to the last implementation (rollback plan) if the install is unsuccessful, including complete backups of previous versions of software and a test of the rollback plan prior to implementation to the production environment;

d) A policy addressing emergency change procedures;

e) Procedures for testing and migration of changes;

f) Segregation of duties between the developers, quality assurance team, the migration team and users; and
g) Procedures to ensure that technical and user documentation is updated as a result of a change.

B.8.3 Software Development Life Cycle

The acquisition and development of new software shall follow defined processes established by the operator and/or DCP.

a) The production environment shall be logically and physically separated from the development and test environments. When cloud platforms are used, no direct connection may exist between the production environment and any other environment.
b) Development staff shall be precluded from having access to promote code changes into the production environment.
c) There shall be a documented method to verify that test software is not deployed to the production environment.
d) To prevent leakage of sensitive information, there shall be a documented method to ensure that raw production data is not used in testing.
e) All documentation relating to software and application development shall be available and retained for the duration of its lifecycle.

B.8.4 Patches

All patches should be tested whenever possible on a development and test environment configured identically to the target production environment. Under circumstances where patch testing cannot be thoroughly conducted in time to meet the timelines for the severity level of the alert and if authorized by the DCP, then patch testing should be risk managed, either by isolating or removing the untested component from the network or applying the patch and testing after the fact.

B.9 Periodic Security Testing

B.9.1 Technical Security Testing

Periodic technical security tests on the production environment shall be performed as required by the DCP to guarantee that no vulnerabilities putting at risk the security and operation of the Electronic Wagering Platform exist. These tests shall consist of a method of evaluation of security by means of an attack simulation by a third-party following a known methodology, and the analysis of vulnerabilities will consist in the identification and passive quantification of the potential risks of the system. Unauthorized access attempts shall be carried out up to the highest level of access possible and shall be completed with and without available authentication credentials (white box/black box type testing). These allow assessments to be made regarding operating systems and hardware configurations, including but not limited to:

a) UDP/TCP port scanning;
b) Stack fingerprinting and TCP sequence prediction to identify operating systems and services;
c) Public Service Banner grabbing;
d) Web scanning using HTTP and HTTPS vulnerability scanners; and
e) Scanning routers using BGP (Border Gateway Protocol), BGMP (Border Gateway Multicast Protocol) and SNMP (Simple Network Management Protocol).

B.9.2 Vulnerability Assessment

The purpose of the vulnerability assessment is to identify vulnerabilities, which could be later exploited during penetration testing by making basic queries relating to services running on the systems concerned. The assessment shall include at least the following activities:

a) External Vulnerability Assessment – The targets are the network devices and servers which are accessible by a third-party (both a person or a company), by means of a public IP (publicly exposed), related to the system from which is possible to access sensitive information.

b) Internal Vulnerability Assessment – The targets are the internal facing servers (within the DMZ, or within the LAN if there is no DMZ) related to the system from which is possible to access sensitive information. Testing of each security domain on the internal network shall be undertaken separately.

B.9.3 Penetration Testing

The purpose of the penetration testing is to exploit any weaknesses uncovered during the vulnerability assessment on any publicly exposed applications or systems hosting applications processing, transmitting and/or storing sensitive information. The penetration testing shall include at least the following activities:

a) Network Layer Penetration Test – The test mimics the actions of an actual attacker exploiting weaknesses in the network security examining systems for any weakness that could be used by an external attacker to disrupt the confidentiality, availability and/or integrity of the network.

b) Application Layer Penetration Test – The test uses tools to identify weaknesses in the applications with both authenticated and unauthenticated scans, analysis of the results to remove false positives, and manual testing to confirm the results from the tools and to identify the impact of the weaknesses.

B.9.4 Information Security Management System (ISMS) Audit

The audit of the Information Security Management System (ISMS) is to be conducted, including all the locations where sensitive information are accessed, processed, transmitted and/or stored. The ISMS will be reviewed against common information security principles in relation to confidentiality, integrity and availability, such as the following sources or equivalent:

a) NIST 800 series Information Security Management Systems (ISMS);

b) Payment Card Industry Data Security Standards (PCI-DSS); and

c) World Lottery Association Security Control Standards (WLA-SCS).

B.9.5 Cloud Service Audit

An operator making use of a cloud service provider (CSP), as allowed by the DCP, to store, transmit or process sensitive information shall undergo a specific audit as required by the regulatory body. The CSP will be reviewed against common information security principles in relation to the provision and use of cloud services, such as NIST 800 series, or equivalent.

a) If sensitive information is stored, processed or transmitted in a cloud environment, the applicable requirements will apply to that environment, and will typically involve validation of both the CSP's infrastructure and the operator's usage of that environment.

b) The allocation of responsibility between the CSP and the operator for managing security controls does not exempt an operator from the responsibly of ensuring that sensitive information is properly secured according to the applicable requirements.
c) Clear policies and procedures shall be agreed between the CSP and the operator for all security requirements, and responsibilities for operation, management and reporting shall be clearly defined and understood for each applicable requirement.