INTEGRITY REQUIREMENTS

Internet Gaming Operating Standard

Saskatchewan Liquor and Gaming Authority

September 21, 2022

Contents

Introduction

The Saskatchewan Liquor and Gaming Authority (SLGA) is responsible for the regulation of gaming in Saskatchewan as mandated under *The Alcohol and Gaming Regulation Act, 1997*. This document outlines the operating requirements for internet gaming processes.

Background

This Internet Gaming Operating Standard (Standard) has been developed by consulting with regulators from British Columbia, Alberta and Manitoba, and with Gaming Laboratories International (GLI). SLGA has adopted language and concepts from:

- Alcohol and Gaming Commission of Ontario (AGCO)
- Canadian Gaming Association, Draft Statements to Accompany GLI 33: Standards for Event Wagering Systems
- Gambling Research Exchange Ontario, (GREO), April 2021 Research Brief: Safer Gambling Implications of Sports Betting Expansion
- GLI Standard Series GLI 33, Standards For Event Wagering Systems, Version 1.1, May 14, 2019.

Purpose

This Standard provides a foundation for policy and process development. It allows flexibility for operators to establish the most efficient and effective way of meeting integrity outcomes. The operator may determine, within the parameters of this Standard, what works best for operations, and focus resources on addressing key risks in a rapidly evolving industry.

IN.1.00 Application and Implementation

IN.1.01 Application

This Standard and all other requirements established by SLGA apply to authorized operators with respect to internet gaming and associated gaming products and offerings. Authorized operators must comply with this Standard in the operation of online gaming.

SLGA may direct the operator or any registered supplier to comply with any additional standards and requirements, as considered necessary to enhance and preserve the integrity of and public confidence in gaming in Saskatchewan.

IN.1.02 Ownership and Control of Internet Gaming Operating Standard

The ownership and control of this document, and all subsequent amendments, rest with SLGA.

IN.1.03 Document Revision and Maintenance

SLGA will conduct periodic reviews of this Standard to identify and address any changes that may be required. SLGA will consult with stakeholders before making any substantive changes to this Standard. Revisions will be forwarded to stakeholders for review and feedback prior to finalization. At any time, stakeholders may submit a request for SLGA to consider changes.

IN.1.04 Other Documents That May Apply

This Standard establishes minimum guidelines for operational and management aspects of internet gaming and has been developed to complement SLGA's integrity requirements contained in the Internet Gaming System Standard (IGSS) and the Internet Gaming Advertising and Marketing Standard (IGAMS).

1.0.00 Registration of Players

1.0.01 Out-of-Province Players

Authorized operators must deny:

a) Registration to any person whose residence is outside of the Province of Saskatchewan
b) Access to registered players who attempt to use their account from outside of the province.

1.0.02 Gaming Employee Players

a) All individuals associated with the conduct and management and operation of online gaming are prohibited from online play
b) All these positions must be approved by SLGA prior to play being allowed.
c) When an employee self-excludes from online gaming, the gaming employee registration will not be affected.

1.1.00 Restrictions

a) The authorized operator shall not offer games that resemble traditional charitable gaming activities, such as bingo, raffles and breakopens
b) The authorized operator shall not offer lottery products
c) All games must be approved by SLGA
d) The use and location of wagering devices (except personal devices) must be approved by SLGA and adhere to relevant SLGA standards
e) Live games restrictions include:
    a. Gaming equipment used for live casino games must be approved by SLGA or by the registrar of the jurisdiction in which the live games originate, and must be certified by an independent testing laboratory
    b. Access to gaming equipment used for live casino games must be restricted and the equipment must be protected from tampering
    c. Live casino dealers must be registered by SLGA or by the registrar of the jurisdiction in which the live games originate
f) Advertising and marketing content must present online gaming in a responsible manner, which means that advertising, marketing materials and communications shall not target high-risk, underage or self-excluded persons to participate, and must adhere to SLGA advertising and marketing standards

1.2.00 Wagers

1.2.01 Wagering Requirements

Authorized operators must ensure:

a) The outcome of the event being wagered on can be documented and verified
b) The outcome of the event being wagered on can be generated by a reliable and independent source
c) The outcome of the event being wagered on is not affected by any other wager.

d) Wagers are allowed only when there is confidence that the event is effectively supervised and risk has been mitigated (e.g., oversight by a sport's governing body)
e) Integrity safeguards are in place for monitoring wagering irregularities to mitigate the risk of match-fixing, cheat-at-play, and other illicit activity that might influence the outcome of wagers
f) Past events (e.g., historical horse racing) have an outcome that is not publicly known or the outcome is masked
g) The event being wagered on conforms to all applicable laws.

1.2.02 Prohibited Events

The following types of sports and events **are prohibited**:

a) Cannot demonstrate integrity in determining the outcome for wagering purposes
b) Involve children or youth or that are marketed to children or youth
c) Involve amateurs, other than elite national and international sporting activities. (For clarity, events that are allowed include sports under the auspices of U-Sports, Canadian Collegiate Athletic Association [CCAA], and National Collegiate Athletic Association [NCAA]).
    i. For clarity, wagering on the activities in the following leagues is prohibited:
        - Junior hockey (e.g., WHL, CHL)
        - Junior football (e.g., Regina Thunder, Kamloops Broncos)
d) Are objectionable, including:
    i. Animal fighting or cruelty
    ii. Human suffering or death, or involve non-consensual violence or injury
    iii. Contravention of human rights legislation
    iv. Illegal activities
    v. Demeaning or cause humiliation, such as contests based on personal appearance, or that are in poor taste
    vi. Involve undue danger to the participants.

1.2.03 Prohibited Event Wagers

The following types of wagers are prohibited:

a) Proxy betting - An individual places a bet on behalf of someone else, with or without authorization
b) Betting Exchanges - Betting options that are similar to securities exchanges, i.e., players buy and sell based on event outcomes, and conduct trades in real-time throughout the event, either to cut their losses or lock in profit.

1.2.04 Allowable Event Wagers

Acceptable event wagering concepts include:

a) In-play – Also called live betting or wagering on a game while it's happening. The odds may adjust as the game progresses

b) Quick cash outs - Gives a bettor the opportunity to close out an active bet before the outcome is decided, for a smaller profit if the wager was winning or smaller loss if the wager was losing
c) Prop betting – A wager on any aspect of a game besides the final score or outcome. Many of the most popular props revolve around the accomplishments of individual players
d) Micro-wagering – Wagering during an event on things that are about to happen in real time. This bet type will settle much faster than a prop bet as the bettor gets the results of the bet almost immediately
e) Novelty betting - Wagering on the outcome of non-sports events, such as political races, award shows, etc.

1.3.00 Wagering Criteria

1.3.01 Odds/Payouts and Prices

There must be established procedures for setting and updating odds/payouts and prices:

a) The method of making wagers must be straightforward and understandable
b) The player must be informed that a wager has or has not been accepted
c) Information must be made available so that the player is clearly informed of the details of the wager prior to making the wager. This includes:
    i. Providing current odds/payouts and prices
    ii. Changing odds/payouts and prices as necessary
d) All selections in a wager must be displayed to the player
e) Wagers on multiple events must be identified as parlays
f) Where the player has placed a wager and the odds, payouts or prices of the wager change prior to confirmation, there must be an option of confirming or withdrawing the wager (with refund of the wager)
g) A player must be able to manually opt out of a wager at any time prior to placing the bet
h) The player must be informed of the period in which wagers can be made on an event or series of events and wagers cannot be placed after the close of the wagering period
i) Players must not be misled about the odds, payouts or any element of a wager
j) All wagers and payouts must be expressed in Canadian currency.

1.3.02 Wagering Rules

Wagering rules refers to any written, graphical, and auditory information provided to the public regarding wagering operations, and must be approved by SLGA:

a) Wagering rules must be clear, complete, unambiguous, and not misleading or unfair to the player
b) The authorized operator must keep a log of any changes to the wagering rules relating to placing wagers
c) If wagering rules are altered for events being offered, all rule changes must be time and date stamped showing the rule applicable in each period. If multiple

rules apply to an event, the authorized operator must apply the rules that were in place when the wager was accepted.

1.3.03 Wagering Content

The following information must be made available to the player:

a) The methods of funding a wager or player account
b) A clear and concise explanation of all fees and commissions (if applicable)
c) The procedures to deal with interruptions caused by the discontinuity of data flow from the network server
d) 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
e) Payout information, including possible winning positions, rankings, and achievements, along with corresponding payouts, for any available wager option
f) Any restrictive features of wagering, such as wager amounts or maximum win values
g) A description of restricted players, including any applicable limitations on wagering (e.g., athletes must not wager on any sports event in which they are participating)
h) The procedures for handling incorrectly posted events, markets, odds/payouts, prices, wagers, or results
i) A wager cancellation policy for voiding or cancelling wagers, which has been approved by SLGA prior to implementation
j) If the odds/payouts are locked in at the time of the wager, or if the odds/payouts may change prior to the commencement of or during the event
k) A description of how odds/payouts may be adjusted for wagers that have odds/payouts fixed at the time the wager, but have atypical winning outcomes (e.g., dead heats), cancelled legs of wagers with multiple events (e.g., parlays)
l) Wagers that are gathered into pools, must have rules for dividend calculation, including the prevailing formula for pool allocations and the stipulations of the event being wagered upon
m) A statement that the authorized operator reserves the right to:
    i. Refuse any wager or part of a wager or reject or limit selections prior to the acceptance of a wager for reasons indicated to the player in these rules
    ii. Close wagering periods under circumstances prescribed by the authorized operator
n) Prizes for combinations involving participants other than solely the first-place finisher, the order of the participants that can be involved with these prizes (e.g., result 8-4-7)
o) Rules for all wagering options and the expected payouts
p) Rules for event cancellation, including the handling of selections wagers with multiple events where one or more portions of the event are cancelled or withdrawn
q) Conditions for a winning wager and the handling of an award in any case where a

tie is possible

r) Payment of winning wagers, including:
   i. Redemption period
   ii. Method for calculation
   iii. Rounding up, down (truncation), true rounding
   iv. Rounding to what level (e.g., 5 cents).

1.3.04 Promotions and/or Bonuses

a) For promotions, bonuses, and advertising, players must be able to access information pertaining to any available promotions and/or bonuses, including how the player is notified of a promotional award or bonus win.
b) Information must be clear and unambiguous, especially where promotions or bonuses are limited to certain events, markets, or if specific conditions apply
c) Materials that communicate gambling inducements, bonuses and credits are prohibited, except on an operator's gaming site and through direct advertising and marketing, after receiving active player consent.

1.3.05 Contests/Tournaments

a) A contest/tournament, which permits a player to either purchase or be awarded the opportunity to engage in competitive wagering against other players, may be permitted with prior approval by SLGA.
b) Rules must be made available to a player for review prior to contest/tournament registration. The rules must include:
   i. All conditions registered players must meet to qualify for entry and advancement through the contest/tournament
   ii. Specific information pertaining to any single contest/tournament, including the available prizes or awards and distribution of funds based on specific outcomes
   iii. The name of the organization (or persons) that conducted the contest/tournament on behalf of, or in conjunction with, the authorized operator (if applicable)
c) Procedures must be in place to record the results of each contest/tournament and made publicly available for the registered players to review for a reasonable period of time.
d) The results of each contest/tournament must be made available upon request. The results include the following:
   i. Name of the contest/tournament
   ii. Date(s)/times(s) of the contest/tournament
   iii. Total number of entries
   iv. Amount of entry fees
   v. Total prize pool
   vi. Amount paid for each winning category.
e) Free contests/tournaments may be considered with SLGA approval

1.3.06 Suspending Wagers

There must be established procedures for suspending wagers (i.e., stop accepting wagers associated with an event). There must be a process to document the suspension with an audit log that includes the date and time of suspension, the reason for the suspension, and the individual(s) who authorized the suspension.

1.3.07 Wager Cancellations

For players to cancel wagers, the following requirements apply:

a) Information regarding the cancellation policy must be available to the player
b) The reason for cancellation must be within policy guidelines
c) Associated transactions must be voided or cancelled according to the authorized operator's cancellation policy
d) There must be appropriate authorizations for all cancellations

1.3.08 Event Based Wagering Periods

Procedures must be in place to ensure the wagering time periods for event-based wagering are controlled.

1.3.09 Results

If the outcome of an event cannot be authenticated (e.g., an external feed is disrupted making the outcome unavailable), there must be:

a) A method to advise players of changes in results that affect betting outcome
b) A policy and procedure for confirming the outcome by a secondary, trusted and approved source
c) A procedure in place to handle changes in outcome (e.g., due to corrections)

1.3.10 Winning Wager Payment

In the event of a failure of the Internet Gaming System (IGS) to process winning wagers, the operator must have policy detailing the method of disbursement.

1.3.11 Virtual Events

Virtual event wagering may be considered and must be approved by SLGA prior to being offered as a gaming option.

2.0.00 Integrity of Online Gaming

Authorized operators must have measures in place to mitigate integrity risk (e.g., detect match fixing or similar activities) and employ investigatory tools and disciplinary processes to detect and respond to fraudulent activity.

2.1.01 Monitoring Procedures for Collusion and Fraud

The authorized operator must take measures designed to reduce the risk of collusion, unlawful and criminal activity or fraud, including having procedures for:

a) Identifying and/or refusing to accept suspicious wagers which may indicate

cheating, manipulation, interference with the regular conduct of an event, or violations of the integrity of any event on which wagers were made
b) Reasonably detecting irregular patterns or series of wagers to prevent player collusion or the unauthorized use of artificial player software
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
d) Logging all relevant activities related to the detection of collusion and cheating.

2.1.02 Independent Integrity Monitors

The authorized operator may employ the use of independent integrity monitors to reduce the risk of collusion, unlawful and criminal activity, or fraud. Monitors can include human resource, technical or third-party solutions.

2.1.03 Anti-money Laundering Policies

The authorized operator must have policies and procedures to support obligations under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) which are implemented and enforced. At a minimum, the authorized operator must:

a) Ensure employees are trained in AML, and that this training is kept up to date
b) Monitor player accounts for opening and closing in short time frames and for deposits and withdrawals without associated wagering transactions
c) Exercise due diligence for aggregate transactions over a defined period
d) Provide copies of all reports filed with Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and supporting records to SLGA upon request
e) Implement policies, procedures and controls that specify times and situations, based on the assessment of risk, where the authorized operator will ascertain and reasonably corroborate a player's source of funds
f) Implement risk-based policies and procedures that provide for escalating measures to deal with players who engage in behavior that is consistent with money laundering indicators, including the refusal of transactions or exclusion
g) Ensure that mechanisms are in place to share information, in a lawful manner, about high-risk or suspicious activities with other authorized operators which may also be subject to similar activity.

2.1.04 Fraudulent Accounts

In circumstances where the authorized operator has determined player accounts are being used in a fraudulent manner, the authorized operator must have a policy for taking appropriate action. This includes:

a) Maintenance of information about any account's activity if fraudulent activity is detected
b) Suspension of any account of a player engaged in fraudulent activity
c) Handling of deposits, wagers, and wins associated with a fraudulent account.

2.1.05 Cancelling, Voiding, and Suspending Wagers

An authorized operator must make available to players, information on its authority to suspend wagering and to void wagers. The authorized operator's decision to suspend or cancel wagering must be reasonable and made in good faith.

2.1.06 Reporting

a) The authorized operator must make available to players, information on how to report activities related to collusion and cheating; the process must be uncomplicated and readily accessible
b) Complaints of cheating, collusion or any other integrity issues must be:
    i. Investigated by the entity that receives the complaint, and
    ii. Escalated through appropriate communication channels where appropriate
c) The authorized operator must report to SLGA all incidents that affect the integrity of the games or system.

2.1.07 Employee Whistleblowing

There must be an independent "whistleblowing" process for employees to anonymously report deficiencies or gaps in the control environment, as well as incidents of possible authorized operator non-compliance of controls, standards and requirements, or the law. Authorized operators must ensure issues raised are addressed in a timely manner.

2.1.08 Oversight

SLGA must have access to IGS reporting and to any other information SLGA deems necessary to ensure compliance with licensing and regulatory requirements, including but not limited to:

a) Internal and external audits of all relevant systems and documentation (including control activities)
b) Independent audits
c) Reports regarding any incident or matter that may affect the integrity or public confidence in gaming, including any actions taken to prevent similar incidents from occurring in the future
d) Reports regarding any public complaints related to integrity and/or compliance with this Standard, including any actions taken to resolve the complaints
e) Reports regarding any incident of non-compliance with the law, standards and requirements or control activities, including any actions taken to correct the cause of non-compliance
f) Periodic reports demonstrating the performance over time of compliance with control activities.

2.1.09 Retention

Information, including logs, related to compliance with the law, this Standard and/or adherence to control activities must be retained in accordance with federal, provincial and organizational requirements.

3.0.00 Third-Party Management

Authorized operators and gaming suppliers are responsible for the actions of third parties with whom they contract for the provision of any aspect of the authorized operator's business. Third parties carry out activities on behalf of the authorized operator as if they were bound by the same laws, regulations, and standards.

3.1.01 Third-Party Services and Products

The authorized operator must have policies and procedures in place to ensure adherence to the following requirements:

a) Accessing, processing, communicating or managing the system and/or its components; adding products or services to the system; and ensuring its components cover all relevant security requirements
b) Reviewing services, reports and records annually
c) Maintaining and improving existing security policies, procedures and controls, must be managed, taking account of the criticality of systems and processes involved and re-assessment of risks
d) Removing access rights of third-party service providers to the system and/or its components upon termination of their contract or agreement or adjusted upon change.

3.1.02 Third-Party Registration with SLGA

SLGA must be advised of any independent third parties under contract for activities related to online gaming. SLGA will assess to determine whether registration as a gaming supplier is required.

4.0.00 Responsible Gaming

The authorized operator must take steps to minimize potential harm and promote a responsible gaming environment.

4.1.01 Policies and Procedures

Authorized operators must establish and implement requirements that will identify and minimize the risks of harm to players including:

a) Training for managers and staff on responsible gambling policies and procedures
b) Having the following information available to players:
    i. How games work and common misconceptions
    ii. Gaming limit options
    iii. Available support services
    iv. Self-exclusion programs.

4.1.02 Self-Exclusion and Breaks in Play

a) Individuals must have the option to take a break in play and access to a formal self-exclusion program
b) The authorized operator must:

i. Provide the option to initiate a short-term break in play
ii. Ensure that once a player initiates a break, no further wagers are permitted during the time-period of the break
iii. Ensure that the self-exclusion registration process includes information about support options
iv. Clearly indicate the terms and conditions of the self-exclusion program, including the player's obligations under the agreement, the consequences of self-exclusion, and the process for returning to play safely
v. Have the player immediately logged out of the account and prevented from logging in for the duration of the exclusion
vi. Take all reasonable steps to prevent any marketing material, incentives, or promotions from being sent to the self-excluded individual for the duration of the self-exclusion period
vii. Transactions, which were made on future events, prior to self-exclusion, will remain in place, so any winnings must be paid out to that individual.
viii. Have a mechanism in place to facilitate the return of the balance of unused funds to a self-excluded individual.

4.1.03 Limit Setting Features

Players must be provided with a method to set gaming limits (financial and time-based) upon registration and at any time after registration.

4.1.04 Excluded Individuals

The authorized operator must develop policies and procedures for prohibited or excluded players and must maintain a list of these individuals and provide it to SLGA every two weeks. Policy must address whether individuals are excluded from online gaming, on-site gaming, or both.

4.1.05 Notification of Deactivation and Dormant Accounts

A policy and process, approved by SLGA, must be in place to ensure that efforts are made to inform players of funds remaining in dormant player accounts.

4.1.06 Unclaimed Funds from Inactive Accounts

A policy and process, approved by SLGA, must be in place to address unclaimed funds from inactive accounts. An account is inactive if the player has not logged into the account for a time-period to be specified by the authorized operator.

4.1.07 Player Election to Deactivate Account

Players may elect to deactivate their player account at any time. The process must be:

a) Obvious and easy to accomplish for the player
b) Occur quickly without unreasonable delays or intrusive messaging designed to impede deactivation.

4.1.08 Operator Deactivation

A player account may be deactivated by the authorized operator. A player account must be deactivated if:

a) The player has been determined to be underage for gaming
b) Illegal activity or criminal association of the player has been discovered
c) The player is deceased.

5.0.00 Peer-to-Peer Games

SLGA may approve peer-to-peer games providing that the authorized operator develops policies and procedures to ensure that the games can be operated in accordance with SLGA regulatory requirements.

6.0.00 Public Trust and Protection of Assets

Assets (e.g., gaming equipment and systems) must be protected and the integrity of customer information and funds must be safeguarded.

6.1.01 Personal Information/Legal Privacy Requirements

It is the responsibility of all operators and third parties to be aware of, adhere to, and meet their obligations under applicable privacy legislation.

6.1.02 Privacy Policy

During the registration process, the player must agree to the privacy policy.

a) The privacy policy must state:
    i. The player personal and location data required to be collected
    ii. The purpose for information collection
    iii. The period in which the information is stored
    iv. Disclosures required to enforce agreements, to comply with regulations, applicable laws and legal processes
    v. An affirmation that measures are in place to prevent the unauthorized or unnecessary disclosure of the information
b) Consent must be:
    i. Achieved through active participation of the player, e.g., a check box or a call-to-action icon
    ii. Acquired prior to any further player account activity occurring.

6.1.03 Game Management Policy

Terms governing play must not be changed during a game session unless the player is made aware of the change before the player places any wagers in the game.

6.1.04 Cryptocurrency

The use of virtual currency is prohibited.

6.1.05 Gaming Site

The gaming site is a physical area for equipment associated with gaming. To maintain the integrity of wagering operations, gaming sites will be subject to SLGA security and audit requirements.

7.0.00 Technology Controls

7.1.01 Control Environment

The authorized operator must have control policies and procedures in place for activities related to maintenance and installation of components that result in changes to the gaming platform. For example, connecting hardware to the gaming platform within a casino. Independent oversight may be exercised by an internal audit body and/or external auditor, as considered appropriate by the authorized operator and/or SLGA.

7.1.02 Management Overrides

Management overrides of the control activities must be clearly documented and made available to SLGA. At a minimum, approval from at least two authorized persons is required in order to override any control activity, and in each instance, the override must be documented and available upon request.

7.1.03 System Operation & Security System Procedures

The authorized operator must document and follow the relevant procedures for the IGS. These procedures must include the following:

a) Procedures for monitoring the critical components and the transmission of data of the entire system, including:
    i. Communication
    ii. Data packets
    iii. Networks
    iv. Components and data transmissions of any third-party services involved
b) Procedures and security policy for the maintenance of all security aspects of the system to ensure secure and reliable communications, including protection from hacking or tampering
c) Procedures for:
    i. Defining security incidents
    ii. Detecting and monitoring breaches
    iii. Documenting and reporting incidents
    iv. Investigating suspected or actual hacking or tampering with the system
    v. Responding to security incidents for resolution
d) Procedures 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 SLGA and documenting the date, time and reason for the malfunction along with the date and time the system is restored and the issue resolved
vi. Voiding or cancelling wagers and pays if a full recovery is not possible.

7.1.04 Physical Location of Servers

All elements related to processing or communicating controlled information, including those comprising the operating environment of the IGS and/or its components must:

a) Be housed in one or more secure location(s) which may be located locally, within a single gaming site, or may be remotely located outside of the gaming site as allowed by SLGA
b) Have sufficient protection against alteration, tampering or unauthorized access
c) Be equipped with a surveillance system as required by SLGA
d) 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
e) Be equipped with controls to provide physical protection against damage from fire, flood, hurricane, earthquake and other forms of natural or manmade disaster
f) Physically located within the boundaries of the Province of Saskatchewan unless otherwise approved by SLGA

7.1.05 Asset Management

The authorized operator must manage asset housing, processing or communicating controlled information, including those comprising the operating environment of the IGS and/or its components. At a minimum, the authorized operator must:

a) Maintain an inventory of all assets related to critical functions or managing sensitive/private data
b) Develop procedures for adding new assets and removing assets from service
c) Implement policies for acceptable use of assets associated with the system and its operating environment
d) Designate an "owner" responsible for:
    i. Ensuring that information and assets are appropriately classified in terms of their criticality, sensitivity, and value
    ii. Defining and periodically reviewing access restrictions and classifications
e) Create procedures to ensure that recorded accountability for assets is compared with actual assets at regular intervals, or when required by SLGA, and conduct appropriate action with respect to discrepancies
f) Implement copy protection to prevent unauthorized duplication or modification of software:
    i. The method of copy protection must be 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 must be individually verified by the methodology approved by SLGA.

7.1.06 Logical Access Control

The authorized operator must have process and procedures to:

a) Ensure each user has individual authentication credentials
b) Delegate individual credentials through a controlled and formal process
c) Maintain an auditable log of all authentication changes and credential changes
d) Track and manage lost or compromised authentication credentials and authentication credentials of terminated personnel
e) Assign, review, modify, and remove access rights and privileges to each user:
    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
f) Identify and flag suspect accounts where authentication credentials may have been stolen
g) Restrict and tightly control utility programs which can override application or operating system.

7.1.07 Verification Procedures

To maintain security and integrity, and to remain in compliance with prevailing regulation, there must be processes for ongoing change management that includes appropriate reporting to the regulator and compliance testing by a gaming lab. The change management process must include:

a) Clear and official communication channels for regulatory review and approval.
b) A risk classification system
c) Strictly enforced source control to ensure only trusted and approved software/changes are implemented and deployed
d) Any required testing with the type of testing and timing for that testing
e) A mechanism that enables timely feedback for the authorized operator, SLGA and gaming lab to facilitate prompt action
f) Engagement of a gaming lab for the performance of any necessary compliance testing, using standardized procedures, lines of communication and schedules.

7.1.08 Electronic Document Retention System

Reports required by this standard 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
    v. Other information that may be used to identify 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 physically secured with all other critical components of the IGS
h) Is equipped to prevent disruption of report availability and loss of data through hardware and software redundancy best practices, and backup processes.

7.1.09 Business Continuity and Disaster Recovery Plan

A business continuity and disaster recovery plan must be in place to recover wagering operations if the IGS's production environment is rendered inoperable. The plan must:

a) Address the method of storing player data and wagering data to minimize loss. If asynchronous replication is used, the method for recovering data must be described or the potential loss of data must be documented
b) Delineate the circumstances under which the recovery plan 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
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.

7.1.10 Cryptographic Controls

A policy on the use of cryptographic controls and encryption key management for protection of information must be developed and implemented.

a) Any player data and/or sensitive information must be encrypted if it traverses a network with a lower level of trust
b) Data that is not required to be hidden, but requires authentication, must use some form of message authentication technique
c) Authentication must use a security certificate from an approved organization
d) The grade of encryption used must be appropriate to the sensitivity of the data
e) The use of encryption algorithms must be reviewed periodically to verify that the

current encryption algorithms are secure

f) Changes to encryption algorithms to correct weaknesses must be implemented as soon as practical, and if no such changes are available, the algorithm must be replaced
g) Encryption keys must be stored on a secure and redundant storage medium after being encrypted themselves through a different encryption method and/or by using a different encryption key.

7.1.11 Remote Access Security

Remote access is defined as any access from outside the system or system network. Remote access security is allowed by the authorized operator and must:

a) Be performed via a secured method
b) Have the option to be disabled
c) Accept only the remote connections permissible by the firewall application and system settings
d) Be limited to only the application functions necessary for users to perform their job duties
e) Include restrictions on:
    i. Remote user administration functionality (adding users, changing permissions, etc.)
    ii. Access to the operating system or to any database other than information retrieval using existing functions.

7.1.12 Remote Access Procedures and Guest Accounts

A procedure for strictly controlled remote access must be established. 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 authorized operator. This remote access must use specific guest accounts which are:

a) Continuously monitored by the authorized operator
b) Disabled when not in use
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.

7.1.13 Firewall Rules Review

Firewall rules must be periodically reviewed to verify the operating condition of the firewall and the effectiveness of its security configuration and rule sets and must be performed on all the perimeter firewalls and the internal firewalls.

7.1.14 Technical Security Testing

Periodic technical security tests on the production environment must be performed to guarantee that no vulnerabilities risk the security and operation of the IGS. The authorized operator must conduct security testing at regular intervals and make the

results available to SLGA upon request.

7.1.15 Vulnerability Assessment

The authorized operator must conduct a vulnerability assessment at regular intervals and make the results available to SLGA upon request. These assessments identify vulnerabilities, which could be later exploited during penetration testing.

7.1.16 Penetration Testing

The authorized operator must conduct penetration testing at regular intervals and make the results available to SLGA upon request. The penetration testing attempts to exploit weaknesses uncovered during the vulnerability assessment. The penetration test must be conducted on:

a) Any publicly exposed applications
b) Systems that host applications responsible for processing, transmitting and/or storing sensitive information.

7.1.17 Information Security Management Audit

An audit of the security protecting sensitive information includes how the information is stored, accessed, processed, and transmitted. The authorized operator must conduct an information security audit at regular intervals and make the results available to SLGA upon request. This audit will be reviewed against common information security principles in relation to confidentiality, integrity and availability, such as the following sources or equivalent:

a) International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 27001 Information Security Management Systems (ISMS)
b) Payment Card Industry Data Security Standards (PCI-DSS) and
c) World Lottery Association Security Control Standards (WLA-SCS).

7.1.18 Cloud Service Audit

Any Cloud Service Provider (CSP) must be audited at regular intervals with the results made available to SLGA upon request. The CSP will be reviewed against common information security principles in relation to the provision and use of cloud services, such as ISO/IEC 27017 and ISO/IEC 27018, or equivalent.