
Internet Gaming Systems Standard



June 30, 2022

Table of Contents

Approval and Revision History.....	Error! Bookmark not defined.
Introduction.....	5
Background.....	5
Purpose	5
IN.1.00 General.....	5
IN.1.01 Ownership and Control of Internet Gaming Systems Standard Document.....	5
IN.1.02 Document Revision	6
IN.1.03 Parameters of Document	6
IN.1.04 Technology.....	6
IN.2.00 Regulatory Requirements.....	6
IN.2.01 Laboratory Testing	6
IN.2.02 Authorized Operator Requirements.....	6
IN.2.03 Other Saskatchewan Standards	7
IN.2.04 Information Systems Security (ISS) Industry Standards.....	7
IN.2.05 Network Security Management.....	7
IN.2.06 Asset Management	7
IN.2.07 Other Documents That May Apply	7
1.0.00 IGS Platform Requirements.....	8
1.1.01 Game Outcome	8
1.1.02 Communications Channel.....	8
1.1.03 IGS Platform – General Statement	8
1.1.04 Shut down and Recovery	8
1.1.05 Wagering Equipment	8
1.1.06 Third Party Hosting.....	9
1.1.07 Disabling of Gambling.....	9
1.1.08 Incomplete Games	9
1.1.09 User Inactivity Timeout	10
1.1.10 Malfunction.....	10
1.1.11 Client Software	10

1.1.12 Data Transmission and Data Storage	10
1.1.13 Control Environment.....	11
1.1.14 Logical Access Control	11
2.0.00 Data Logging Requirements.....	12
2.0.01 General Requirements.....	12
2.0.02 Player Account Information	12
2.0.03 Gaming Session Information.....	13
2.0.04 Game Information	13
2.0.05 Significant Events Information	13
3.0.00 Administrative Requirements.....	14
3.1.00 Player Registration and Account Requirements	14
3.1.01 Agreement	14
3.1.02 Verification.....	14
3.1.03 Challenge Questions.....	14
3.1.04 Under-Age Persons.....	14
3.1.05 Player Accounts	15
3.1.06 Security.....	15
3.1.07 Player Funds Maintenance	15
3.1.08 Transaction Log or Account Statement.....	16
3.1.09 Unclaimed Funds from Inactive Accounts	16
3.2.00 Anti-Money Laundering (AML) Requirements	16
3.2.01 General Statement	16
3.2.02 Internal Control Procedures.....	17
3.2.03 AML Monitoring	17
3.3.00 Player Protection Requirements	17
3.3.01 General Information	17
3.3.02 Last Login Time Display.....	18
3.3.03 Security Information	18
3.3.04 Session Duration Reminders	18
3.3.05 Time-Based Session Reminders.....	18

3.3.06 Game-Based Session Reminders	19
3.3.07 Player Game Session Finish	19
3.3.08 Self-Exclusion	19
3.3.09 Involuntary Exclusion	20
3.3.10 Self-Limitation	20
3.3.11 Imposed Limitations	20
4.0.00 Software Requirements.....	21
4.1.01 General Statements	21
4.1.02 Choice of RNG	21
4.1.03 Hardware-Based RNGs	21
4.1.04 Software-Based RNGs	21
4.1.05 Scaling.....	21
4.1.06 Period.....	21
4.1.07 Range.....	22
4.1.08 Seeding/Re-Seeding.....	22
4.1.09 Background Cycling/Activity.....	22
4.1.10 Unpredictability	22
4.1.11 Cryptographic RNG	22
4.2.00 Game Behavior Requirements.....	23
4.2.01 Game Fairness	23
4.2.02 Game Play Duration	23
4.2.03 No Adaptive Behavior by Games.....	24
4.2.04 No Forced Game Play	24
4.2.05 Game Play Requirements	24
4.2.06 Game Design	24
4.2.07 Mapping.....	25
4.2.08 Game Play	25
4.2.09 Game Artwork (Information Displayed).....	26
4.2.10 Instructions and Information	27
4.2.11 Bet Display	27

4.2.12 Result Display	28
4.2.13 Game-Specific Requirements	28
5.0.00 Player Location Requirements.....	29
5.1.01 General Statements	29
5.1.02 Fraud Prevention	29
5.1.03 Detection on a Private Network	29
5.1.04 Detection on a Public Network.....	29
6.0.00 Progressive Jackpots	30
6.1.00 Progressive Jackpot Game Requirements.....	30
6.1.01 General Statements	30
6.1.02 Progressive Jackpot Fairness	30
6.1.03 Notification of the Progressive Jackpot Amount	30
6.1.04 Progressive Jackpot Win Notification	30
6.1.05 Progressive Jackpot Parameter Changes.....	30
6.1.06 Multiple Progressive Jackpot Winners	31
6.1.07 Conversion of Progressive Jackpots	31
6.1.08 Progressive Jackpot Financial Liability	31
6.1.09 Progressive Jackpot Shutdown	31
6.1.10 Progressive Jackpot Meters	31
6.1.11 Progressive Jackpot Recovery	31
6.1.12 Progressive Jackpot Controller	31
7.0.00 Software Validation.....	33
7.1.01 Monitoring.....	33
7.1.02 Change Management	34
Definitions	34

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 integrity requirements for Internet Gaming Systems (IGS).

Background

This Internet Gaming Systems 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:

- Alberta Gaming Liquor and Cannabis (AGLC), AGLC Technical Standards For Interactive Gambling, January 2021
- British Columbia Gaming Policy and Enforcement Branch (GPEB), Technical Standards for Internet Gambling Systems, Technical Standards Document (TSD) Version 2.2
- Canadian Gaming Association (CGA), Standards for IGSs, November 2020
- GLI Standard Series GLI-19, Standards For Interactive Gaming Systems, Version 3.0, July 17, 2020
- GLI Standard Series GLI-33, Standards For Event Wagering Systems, Version 1.1, May 14, 2019.

Purpose

This Standard is intended to provide regulatory guidance to manufacturers, suppliers and authorized operators regarding internet gaming technical integrity requirements in Saskatchewan:

- a) To eliminate subjective criteria in analyzing and certifying IGS operations
- b) To create standards that will help ensure that an IGS operating in a live environment is fair, honest, secure, safe, auditable, and able to operate correctly
- c) To recognize that non-gaming testing (such as electrical testing) is not incorporated into this Standard, but left to appropriate test laboratories that specialize in that type of testing
- d) To recognize that, except where specifically identified in this Standard, testing is not directed at health or safety matters. These matters are the responsibility of the manufacturer of the equipment
- e) To ensure requirements can be easily changed or modified to allow for new technology or functionality
- f) To ensure this Standard allows for a wide range of methods and technologies to be used for compliance, while at the same time, to encourage the development of new methods and technologies
- g) Where variations from this Standard are proposed, SLGA will review to determine acceptable practices.

IN.1.00 General

IN.1.01 Ownership and Control of Internet Gaming Systems Standard Document

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

IN.1.02 Document Revision

Technological change in the industry may require SLGA to issue corresponding amendments and changes to previously approved standards. Reasonable notice will be given to all manufacturers, suppliers, testing laboratories, and operators for implementation.

IN.1.03 Parameters of Document

This document outlines those requirements that apply to the IGS to create a standard which will ensure that the IGS is fair, secure and has the capability to be audited and operated in accordance with SLGA regulatory requirements.

- a) Corresponding policies created by the operator must be consistent with this Standard and approved by SLGA prior to implementation
- b) Any games or new game concepts added to the IGS must be approved by SLGA prior to implementation.

IN.1.04 Technology

One should be cautioned that this Standard should not be read in such a way that limits the use of future technology. This Standard should not be interpreted that if the technology is not mentioned, then it is not allowed. As new technology is developed, SLGA, in consultation with the authorized operator, will review and make any changes deemed necessary, and incorporate new minimum standards for the new technology.

Although an authorized operator may recommend that particular changes be made to this Standard, the ultimate authority to approve changes rests solely with SLGA.

IN.2.00 Regulatory Requirements

IN.2.01 Laboratory Testing

An IGS must be tested and certified by a qualified, independent testing laboratory that is registered with SLGA.

- a) SLGA reserves the right to determine:
 - i. What constitutes an IGS
 - ii. Which products require testing
- b) Before being permitted to operate in the live environment available to the public, all IGS components must be tested to applicable Saskatchewan standards
- c) Final testing and evaluation results, reports, and any additional documentation as may be required, must be submitted directly to SLGA.

IN.2.02 Authorized Operator Requirements

The authorized operator of an IGS must:

- a) Follow all the terms and conditions for applicable online games
- b) Have all policies and procedures related to IGS operations approved by SLGA prior to system deployment in a live environment
- c) Assist regulatory personnel to perform internal quality assurance testing on an IGS as determined by SLGA.

IN.2.03 Other Saskatchewan Standards

A standard is rarely applied in isolation. This Standard establishes minimum guidelines for operational and management aspects of an IGS and has been developed to complement SLGA's integrity requirements contained in the Internet Gaming Operating Standard (IGOS).

When gaming components are integrated to create an IGS, additional technical standards will be required. In this regard, standards are complementary and, in circumstances where there is uncertainty regarding specific testing requirements, SLGA will review each situation and engage in discussions with the testing laboratory and manufacturer to determine which additional standards require inclusion in the testing and certification process.

IN.2.04 Information Systems Security (ISS) Industry Standards

SLGA specifies the requirements for establishing, implementing, maintaining and continually improving information security management processes within the context of any products submitted for testing. Aspects of products that fall outside the realm of testing by the laboratory are subject to assessment and treatment of information security risks tailored to the design and functionality of the product. These subsequent requirements set out by SLGA are generic and are intended to be guiding principles for all IGS related products.

IN.2.05 Network Security Management

The Administrative Controls, Technical Controls and Physical & Environment Controls for the IGS should incorporate the best practice principles found in the applicable and relevant ISS industry standards, as dictated by, but not limited to, sources such as:

- a) ISO/IEC 27001 – Information Security Management Systems (ISMS)
- b) ISO/IEC 27002 – Code of practice for information security management
- c) ISO 31000:2009 - Risk Management – Principles and guidelines
- d) Open Source Security Testing Methodology Manual (OSSTMM).

Other normative references will be considered by SLGA on a case-by-case basis.

IN.2.06 Asset Management

All assets housing, processing or communicating controlled information, including those comprising the operating environment of the IGS and/or its components, will be:

- a) Managed according to security management practices to ensure that information and assets are appropriately classified, protected and monitored with processes established for periodically reviewing access restrictions and classifications
- b) Contained in a secure, controlled physical location with access to the IGS limited to authorized personnel
- c) Physically located within the boundaries of the Province of Saskatchewan unless otherwise approved by SLGA.

IN.2.07 Other Documents That May Apply

Technical and operational information, directly relevant to the system being submitted for testing, must be provided at SLGA's request.

1.0.00 IGS Platform Requirements

1.1.01 Game Outcome

All critical functions, including the result of any game and the associated payout, must be generated by the IGS and be independent of the end player device (i.e., end user) except for the player's selections/choices during game play.

1.1.02 Communications Channel

Where the game outcome is derived from a random number generator (RNG), that outcome must not be affected by the effective bandwidth, link utilization, bit error rate or other characteristics of the communications channel between the IGS and the end player device.

1.1.03 IGS Platform – General Statement

If the IGS is comprised of multiple computer systems at various sites, the IGS as a whole, and all communication between its components, must conform to these requirements.

1.1.04 Shut down and Recovery

- a) The IGS must be able to perform a graceful shutdown (i.e., a shutdown where no data is lost, and all applications are able to close properly) in the event of a simple power failure, and not restart automatically on power up
- b) In the event of a critical hardware/software failure, the IGS must have the ability to initiate a recovery of all critical information from the time of the last backup to the point in time at which the system failure occurred
- c) The authorized operator must have disaster recovery capability in place that is sufficient to ensure player entitlements are protected and audit capability is facilitated up to the point of the disaster
- d) The IGS must be able to recover from unexpected restarts of its central computers or any of its other components.

1.1.05 Wagering Equipment

The authorized operator shall provide a secure location for the placement, operation, and usage of wagering equipment with appropriate security policies and procedures to ensure that risks are identified, mitigated and underwritten by contingency plans. In addition:

- a) Wagering equipment shall be situated to reduce the risks from:
 - i. Environmental threats and hazards
 - ii. Opportunities for unauthorized access
 - iii. Power failures
 - iv. Other disruptions caused by failures in supporting utilities
- b) Only authorized individuals will have access to the wagering equipment
- c) It shall not be possible to modify the configuration settings of the wagering equipment without a secure, authorized process
- d) Where supported, the wagering equipment shall provide a means to record the following audit information:
 - i. All available employee privileges related to the configuration of the wagering equipment associated with the user account
 - ii. Auto-lockout of employee activity after a determined time limit (e.g., 5 minutes) that requires re-establishment of their login in order to continue

- e) To ensure its continued availability and integrity, processes shall be implemented for wagering equipment to be properly maintained, inspected and serviced at regular intervals
- f) Prior to disposal or re-use, wagering equipment shall be checked to ensure that any licensed software, player account information, and other sensitive information has been removed or securely overwritten (i.e., not just deleted)

1.1.06 Third Party Hosting

Where one or more components of the IGS are hosted by a third party service provider, the following requirements must be met:

- a) The private and financial information of all players must be protected by the third party service provider using industry-standard ISS controls
- b) No third party service may be used which requires software to comply with rules/regulations which are contradictory to any items found within this Standard.

1.1.07 Disabling of Gaming

- a) The IGS must provide a mechanism for all gaming offered on the IGS to be disabled, as a whole or individually, by the authorized operator
- b) The IGS must provide a mechanism for each active game session on the IGS to be disabled individually by the authorized operator
- c) When a game is disabled, all players playing that game must be permitted to conclude their current game in play:
 - i. Presently, or
 - ii. When that game next becomes available to the player
- d) Once a game is disabled, it must not be accessible to players
- e) The IGS must provide full audit trails when disabling a game that is currently in play

1.1.08 Incomplete Games

- a) The IGS must provide a mechanism for a player to complete an incomplete game before a player is permitted to participate in another instance of the same game. Incomplete games include:
 - i. Loss of communications between IGS and end player device
 - ii. IGS restart
 - iii. Game disabled by IGS
 - iv. End player device restart
 - v. Abnormal termination of gaming application on end player device
- b) Bets associated with a partially complete game that can be continued must be held by the IGS until the game completes. Player accounts must reflect any funds held in incomplete games
- c) The IGS must provide clear notification to the player, either through the game help/rules screen and/or the IGS terms & conditions, that bets placed but remaining undecided in incomplete games (i.e., without the player returning to that game in order to complete it) beyond a stipulated timeframe, will become void. The notification must include the criteria under which an undecided bet will be voided, and the process used to void the bets.

1.1.09 User Inactivity Timeout

- a) The IGS must allow the authorized operator to implement a user inactivity timeout based in minutes. The default inactivity time period shall not exceed 30 minutes
- b) If a session is terminated due to a user inactivity timeout, the end player device must display to the player the server session termination (i.e., the user inactivity timeout) upon the player's next attempted action on the IGS. No further game play is permitted until the IGS and the end player device establish a new session.

1.1.10 Malfunction

The IGS must not be affected by the malfunction of end player devices other than to institute the incomplete games procedures in accordance with these requirements:

- a) Any unrecoverable malfunction of gaming hardware/software must result in the voiding of affected game bets and pays, and the return of affected bets
- b) The terms and conditions of game play must clearly define the rules by which these unrecoverable malfunctions of gaming hardware/software are addressed.

1.1.11 Client Software

Where wagering is conducted through the use of client software installed on the end player device, the following requirements apply to that client software and the client-server interactions:

- a) The client software must not be allowed to automatically alter any firewall rules to open ports that are blocked by either a hardware or software firewall
- b) The client software must not access any ports which are not necessary for the communication between the client and the server
- c) The client software installation instructions must not require or instruct the end user to manually open up any ports on their firewall for any port that is not directly used in client-server communications
- d) Players must not be able to use the client 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.), and all data transferred in this manner must be:
 - i. Automatically scanned for viruses or other malicious content (where appropriate)
 - ii. Logged by the IGS
- e) If the client software includes additional non-gaming related functionality, this additional functionality must not alter the game's integrity in any way.

1.1.12 Data Transmission and Data Storage

- a) Where player personal information is being passed over communication lines, or being stored within the IGS, such data must be protected with measures commensurate with the sensitivity of that data and in compliance with applicable privacy legislation
- b) Examples of player personal information include:
 - i. Player name
 - ii. Player email address
- c) Examples of sensitive player personal information that require advanced protection measures, such as encryption (or other commensurate controls) include:
 - i. Player identity details (including player identity verification results)
 - ii. Player physical address and contact numbers
 - iii. Credit and debit card details

- iv. PINs and passwords
 - v. Account details and balances
 - vi. Player protection limitations
 - vii. Player protection exclusions
 - viii. Money transfers to and from player accounts
 - ix. Changes to account details, such as change of address, change of credit card, or change of name
 - x. Game play (e.g., games played, amounts bet, amounts won)
- d) Any sensitive or confidential information maintained by the IGS must be stored in areas of the system that are secured from unauthorized access, both external and internal.

1.1.13 Control Environment

By means of logging, reporting and security features (or any combination thereof), the IGS must be capable of supporting the following requirements:

- a) Management overrides
- b) Information technology asset management practices
- c) Appropriate access controls
- d) Electronic documentation retention processes
- e) Robust fail-over and redundancy for business continuity and recovery
- f) Cryptographic controls
- g) Security controls for authorized remote access
- h) Guest accounts
- i) Security testing
- j) Audits.

1.1.14 Logical Access Control

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

- a) Each user shall have an 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) 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
- f) The system shall generate a flag for suspect accounts where authentication credentials may have been stolen
- g) Any logical access attempts to the system applications or operating systems shall be recorded in a secure log.

2.0.00 Data Logging Requirements

2.0.01 General Requirements

- a) The IGS must be capable of retaining and backing up all recorded information for as long as the period required by SLGA and federally legislated authorities, based on the type of information (e.g., FINTRAC)
- b) The number of digits to be used in all fields must be based on appropriately projected performance and business
- c) Storage of archived data may reside outside of the core IGS
- d) All implemented time stamping recorded information must make use of the 24-hour format. All times displayed to players must be the current time for Saskatchewan's time zone
- e) All date stamping implemented throughout recorded information must make use of a consistent format to be prescribed by the authorized operator
- f) Where different transaction server processes write to the same transaction log, it must be possible to identify the originating server for each transaction.

2.0.02 Player Account Information

- a) For each individual player account, the IGS must maintain and back up the following information, and be capable of reporting this information to the authorized operator for the authorized operator-configurable time span, upon request:
 - i. Player identity details (including player identity verification results)
 - ii. Account details and current balance
 - iii. Changes to account details, such as change of address, change of credit card, or change of name
 - iv. Any self-imposed player protection limitations
 - v. Any self-imposed player protection exclusions
 - vi. Details of any previous accounts, including reasons for deactivation
 - vii. Deposit/withdraw history
 - viii. Game play history or wager history (e.g., games played, amounts bet, wagers placed, amounts won, Progressive Jackpots won, etc.)
- b) For player accounts as a whole, the IGS must be capable of generating the following reports for the authorized operator-configurable time span upon request:
 - i. A list of all currently (or previously) active player accounts
 - ii. A list of all currently (or previously) inactive player accounts (including reasons for deactivation)
 - iii. A list of all accounts for which the player has currently (or previously) imposed a player protection self-exclusion
 - iv. A list of all accounts for which the player has currently (or previously) been excluded from the site by the authorized operator (e.g., involuntary exclusion)
 - v. A list of all accounts for which the player's funds have currently (or previously) been inactive for a period of time exceeding 90 days
 - vi. A list of all accounts for which one or more of the player's deposits and/or withdrawals have exceeded any authorized operator-configurable limit (e.g., large deposits/withdrawals). The limit must be configurable for single transactions, as well as aggregate transactions, over an established time period
 - vii. A list of all accounts for which one or more of the player's wins have exceeded any

authorized operator-configurable limit (e.g., large wins). The limit must be configurable for single wins, as well as aggregate wins, over an established time period.

2.0.03 Gaming Session Information

- a) For each individual gaming session, the IGS must maintain and back up the following information, and be capable of reporting this information to the authorized operator:
 - i. Unique player ID
 - ii. Gaming session start and end time
 - iii. Game play or wager information for session (e.g., games played, amounts bet, amounts won, Progressive Jackpots won, etc.)
- b) For gaming sessions as a whole, the IGS must be capable of generating the following report upon request:
 - i. A list of all currently active gaming sessions.

2.0.04 Game Information

For each individual game played or wager placed, the IGS must maintain and back up the following information, and be capable of reporting this information on demand in a format configurable by the authorized operator:

- a) Unique player ID
- b) Unique game identifier
- c) Start time, according to IGS
- d) Player account balance at start of game
- e) Amount wagered
- f) Contributions to Progressive Jackpot pools
- g) Current game status (i.e., in progress/complete) (note: the IGS must maintain records of any game that fails to complete, and the reason why the game failed to complete)
- h) Game result/outcome
- i) Progressive Jackpot wins
- j) Game end time, according to IGS
- k) Amount won
- l) Player account balance at end of game
- m) Approved game/pay table versions.

2.0.05 Significant Events Information

- a) The IGS must maintain and back up the following information, and be capable of reporting this information on demand and in a format configurable by the authorized operator:
 - i. Changes made by the authorized operator to game parameters (note: for the purposes of sports wagering, which can implement dynamic odds/payouts setting, only the odds/payouts actually used for each individual wager need to be retained)
 - ii. Changes made by the authorized operator to Progressive Jackpot parameters
 - iii. New Progressive Jackpots created
 - iv. Progressive Jackpot wins
 - v. Progressive Jackpot shutdowns.

3.0.00 Administrative Requirements

3.1.00 Player Registration and Account Requirements

3.1.01 Agreement

Part of the player's registration process must be an agreement to the terms and conditions of game play.

- a) Where player devices (i.e., end user) utilize mobile technologies (which tend to implement miniature screens), it is permissible to present the check box or acceptance button outside of the terms and conditions, provided that the terms and conditions are made available to the player (e.g., through some form of link) should the player choose to review the terms and conditions before acceptance
- b) The players can only advance to "cash" play if they take an action to acknowledge the agreement.

3.1.02 Verification

- a) Players must register with the operator before commencement of gaming
- b) The authorized operator's IGS registration process must be capable of confirming the identity, age and address of a player before permitting creation and activation of a valid player's account:
 - i. The IGS must deny registration to under-aged persons
 - ii. The IGS must deny registration to persons whose address is outside of the Province of Saskatchewan
- c) The IGS must deny registration to persons who are identified as having self-excluded until such time as the self-exclusion has been revoked
- d) The IGS must deny registration to persons who are not permitted to create an account by reason of a prohibition issued by the authorized operator (e.g., involuntary exclusion or impermissible bettors)
- e) Initial player access, or initial access from an unrecognized device to the IGS, must utilize multi-factor authentication methods that also involve at least a user ID and password
- f) Initial passwords are set by the player; however, any subsequent password resets must be issued in a secure manner.

3.1.03 Challenge Questions

- a) Players must be asked to nominate a number of challenge questions (and answers) at the time of registration
- b) These questions must be used by the IGS (or help-desk staff) if a password or PIN is forgotten to identify the person requesting to access the account or change the password.

3.1.04 Under-Age Persons

- a) No bets shall be accepted from a player unless that person has been registered and confirmed as a player who is 19 years of age or older
- b) The IGS must be capable of generating a detailed report of any player's activity such that if a player is ever found to be underage, the authorized operator has all of the necessary information to take whatever action is deemed appropriate by the authorized operator.

3.1.05 Player Accounts

A new player must be registered prior to creating an account:

- a) A new player must create an account in order to deposit funds for game play
- b) A player must only be permitted to have one active account at a time
- c) Depositing funds will be by a method acceptable to the authorized operator and made known to the player on the player account payment screen
- d) A new account for a person must not be created if a previous account indicates that the person must not be permitted to establish another account.

3.1.06 Security

- a) Player accounts on the IGS must be secured against unauthorized access or update other than by approved methods. This includes internal access by the authorized operator staff, and external access by unauthorized parties
- b) In the case of mobile gaming, encrypted HTTPS (or equivalent) is sufficient for the wireless communication of any sensitive player personal information
- c) The authorized operator shall include in the terms and conditions a notification that players are responsible for the security aspects of their end-player device.

3.1.07 Player Funds Maintenance

- a) All transactional data, including deposits with authorization numbers (or equivalent, as provided by the financial institution/payment system), withdrawals, transfers or adjustment transactions, must be maintained in a system audit log.
 - i. Transactional data need only be maintained by the IGS for as long as the period required by relevant provincially and/or federally legislated authorities, based on the type of information
 - ii. Transactional data archiving is permitted
- b) Except where rules within the player agreement and/or prize payout policies impose additional requirements prior to a payout being made, a player must be able to withdraw for play, funds up to the current balance of their account at any time
- c) Inactive accounts holding monies in the IGS must be protected against forms of illicit access or removal. This includes unauthorized internal access by the authorized operator staff, and external access by unauthorized parties
- d) System withdrawals during play from a player's account on the IGS cannot be paid back to a credit card, except where a credit card transaction error requires correction, or where a deposit refund is required, in which case, a void or refund credit card transaction process for the same value as the original transaction can be used
- e) System payments to a player's account must either be paid directly to an account with a financial institution that is specifically named by the player through the course of configuring their player account on the gaming platform, or made payable to the player and forwarded to the player's address. The name and address must be the same as held in the player registration details
- f) The IGS must be capable of identifying where the same financial institution account number is listed in two or more separate player accounts
- g) Any funds left in a player's account that is to be de-activated are to be remitted in the name of the owner of the account
- h) The IGS must not permit the withdrawal of funds for play, in excess of the player's balance

- i) If a player initiates a financial transaction and that transaction would exceed limits put in place by the authorized operator and/or SLGA, this transaction may only be processed provided that the player is clearly notified that funds withdrawn or deposited are less than requested
- j) It shall not be possible to transfer funds between two player accounts.

3.1.08 Transaction Log or Account Statement

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

- a) Financial Transactions (time stamped with a unique transaction ID):
 - i. Deposits to the player account
 - ii. Withdrawals from the player account
 - iii. Incentive credits added to/removed from the player account (outside of credits won in a game)
 - iv. Manual adjustments or modifications to the player account (e.g., due to refunds)
 - v. Any non-wager purchases (if applicable)
- b) Game History (by game theme)
 - i. The name of the game theme and game type (reel, blackjack, poker, table, etc.)
 - ii. Total amount wagered, including any incentive credits (if applicable)
 - iii. Total amount won for completed games, including, any incentive credits and/or prizes, and any Progressive Jackpots and/or incrementing jackpots (if applicable)
- c) Transaction activity reports will be available:
 - i. Online through their player account, or
 - ii. By request to the authorized operator

3.1.09 Unclaimed Funds from Inactive Accounts

The IGS must support processes developed to deal with unclaimed funds from inactive accounts. An account is considered to be inactive if the player has not logged into the account for a time period specified by the authorized operator.

3.2.00 Anti-Money Laundering (AML) Requirements

3.2.01 General Statement

The authorized operator must ensure that the IGS is capable of the following:

- a) Closing player accounts
- b) Imposing deposit and/or win limits on players
- c) Cancelling, voiding, and suspending wagers
- d) Logging and reporting player account activity, including:
 - i. Opening and closing in short time frames
 - ii. Deposits and withdrawals without associated game play
- e) Distinguishing between deposits and wins

3.2.02 Internal Control Procedures

The IGS shall provide functionality and reporting ability to support the authorized operator with establishing, maintaining, implementing and complying with internal control procedures for player account operations and financial transactions. The IGS shall support the following internal controls for risk that includes, but is 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 AML compliance standards including procedures for detecting structuring to avoid reporting requirements
- f) Description of all software applications that comprise the IGS
- g) Description of all integrated third-party service providers
- h) Any other information required by SLGA.

3.2.03 AML Monitoring

The IGS shall provide functionality and reporting to support AML procedures and policies implemented by the authorized operator to ensure:

- a) Transactions are monitored for funds transferred from one player account then transferred to another player account
- b) Player accounts are monitored for opening and closing in short time frames and for deposits and withdrawals without associated game play transactions
- c) Aggregate transactions for a player account over a defined period are monitored to determine if further due diligence checks are required and reportable to the relevant organization if they exceed an established threshold
- d) Identification of a player and the player's source of funds for purposes of anti-money laundering requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PC(ML)TFA), including any risk assessments or reporting requirements, its regulations and guidance from the Financial Transactions and Reports Analysis Centre (FINTRAC), and any requirements observed by SLGA, in order to trigger an appropriate response by the authorized operator
- e) Unless authorized by SLGA, the IGS does not permit the use of virtual currency.

3.3.00 Player Protection Requirements

3.3.01 General Information

- a) The authorized operator shall ensure that the IGS website complies with:
 - i. Applicable provincial advertising and marketing standards
 - ii. Approved responsible gaming policies
- b) The gaming platform must provide the player with an easily accessible mechanism to view responsible gaming. For example: a link to a separate page containing the information, or responsible gaming information available within individual games themselves.
- c) The responsible gaming information must contain, at a minimum:
 - i. The province's current responsible gaming message
 - ii. A link to an approved responsible gaming website
 - iii. Information about potential risks associated with gaming, and where to get help

- iv. Meaningful and accurate information about games and gaming (in general)
- v. Rules of play
- vi. Percentage Return to Player (%RTP) values, commission, and odds of winning, or odds/payouts
- vii. Information about self-exclusion programs
- viii. A link to the terms and conditions the player agreed to be bound to under any player agreement and by entering and playing on the site
- ix. A link to the authorized operator privacy policy
- d) Account related windows on the site (particularly the deposit window) must provide a readily accessible link to the player protection/responsible gaming page
- e) The player protection/responsible gaming page must be readily accessible from any screen available where game play may occur. Note: for the purposes of end player devices that utilize mobile technologies (which tend to implement miniature screens), the link to the player protection/responsible gaming page may be represented by a reasonably sized graphic, text, logo or symbol.
- f) The authorized operator must address the possibility of the game being won (or appearing to be won) by one or more players simultaneously. The rules of the game must include resolution of this possibility.

3.3.02 Last Login Time Display

When a player logs into the IGS, the last time they logged in must be displayed.

3.3.03 Security Information

- a) The rules of play must advise the player to keep their password and login ID secure
- b) The rules of play must advise the player to be aware of what mechanisms exist to detect if there is unauthorized use of their account, such as observing the last login time display, and reviewing credit card statements against known deposits.

3.3.04 Session Duration Reminders

- a) The IGS must employ a session duration reminder function for all games offered on the IGS, except as noted in subsection (c) below
- b) The method of reminder notification and the trigger method used to invoke the reminder may differ based on the type of game being played
 - i. The duration trigger may be time-based, and either player-configurable or automatic
 - ii. The duration trigger may be game-based, and automatic (i.e., not configurable by the player)
- c) Session duration reminders are not required for games where the player only wagers on a future event such as with sports wagering or periodic lottery draws.

3.3.05 Time-Based Session Reminders

- a) Where the game being played implements a time-based trigger, it may either be player-configurable or automatic:
 - i. For the player-configurable option, before being permitted to play, the player must be required to choose a timeframe for session duration reminders. The available options for timeframes for session duration reminders must include one hour, four hours, and at least one value in between. It is acceptable for this choice to include a default option for the player to select

- ii. For the automatic (i.e., not configurable by the player) option, the system must implement the shortest duration of time (i.e., one hour)
- b) During a session, after the specified timeframe has elapsed, a message must appear on the screen clearly advising the player how long they have been playing. The message must:
 - i. Be displayed immediately
 - ii. Be displayed immediately upon completion of the current game or tournament in progress, or
 - iii. Be displayed immediately upon the player's next interaction with the game or website
- c) Once the message has been displayed, the player must be required to take special action to continue gaming, such as checking a box or selecting an acceptance button
- d) Thereafter, where the player chooses to continue gaming, upon each subsequent cycle of the specified timeframe, steps b) and c) above must be repeated.

3.3.06 Game-Based Session Reminders

- a) Where the game being played implements a game-based trigger (i.e., a trigger based on the number of completed games within the same session), the number of completed games between session duration reminders will be determined by the authorized operator in consultation with and as approved by SLGA. Where no specific agreement exists, the default trigger amount shall be no greater than the maximum number of games that can be played within the shortest duration of time
- b) During a session, once the number of completed games has reached the trigger threshold, a message must appear on the screen clearly advising the player that they have played the number of games set for the session reminder. The message must either:
 - i. Be displayed immediately upon completion of the current game or tournament in progress
 - ii. Be displayed immediately upon the player's next interaction with the game or website
- c) Once the message has been displayed, the player must be required to take special action to continue gaming, such as checking a box, or selecting an acceptance button,
- d) Thereafter, where the player chooses to continue gaming, upon each subsequent cycle of the completed games trigger, steps b) and c) above must be repeated.

3.3.07 Player Game Session Finish

A session finishes if:

- a) The player chooses to terminate play and notifies the IGS that the session is finished (e.g. logs out)
- b) A player-inactivity timeout is reached, or
- c) The authorized operator terminates the session.

3.3.08 Self-Exclusion

- a) Players must be provided with an easy and obvious mechanism to self-exclude from game play
- b) At a minimum, this self-exclusion mechanism must be accessible from the player protection/responsible gaming page. Note: the player must be logged into their account in order to activate the mechanism
- c) The player must be provided with the option to self-exclude for a specified period of time as defined in the Player Agreement. The IGS must ensure that:

- i. Immediately upon receiving the self-exclusion order, no new bets or deposits are accepted from that player, until such time as the temporary self-exclusion has expired
- ii. Player wins may be processed during the self-exclusion period, provided that the originating wager was placed prior to the receipt of the self-exclusion order
- iii. During the self-exclusion period, the player is not prevented from withdrawing any or all of their account balance, provided that the system acknowledges that the funds have cleared
- d) In the case of a self-exclusion, a player must not be permitted to establish another account until the time period of exclusion has elapsed.

3.3.09 Involuntary Exclusion

- a) The IGS must provide a mechanism by which the authorized operator staff can exclude a player from the IGS under the terms of any player agreement
- b) Immediately upon activating the exclusion, no new bets or deposits are to be accepted from that player, until such time as the exclusion has been revoked
- c) During the exclusion period, the player must not be prevented from withdrawing any or all of their account balance, provided the system acknowledges that the funds have cleared, and that the reason(s) for exclusion would not prohibit a withdrawal.

3.3.10 Self-Limitation

- a) The IGS must provide players with an easy and obvious mechanism to self-limit their game play
- b) At a minimum, this self-limitation mechanism must be accessible from the player protection/responsible gaming page
- c) Immediately upon receiving any self-limitation order, the IGS must ensure that all specified limits are correctly implemented in the system
- d) It is acceptable that self-limitations take effect the next time that the player logs into the IGS; however, the player must be clearly informed that this is the case upon setting the limit
- e) Once established by a player, it must only be possible to reduce the severity of self-limitations with 24 hours' notice
- f) Self-limitations must not be compromised by external time events, such as leap-years
- g) Self-limitations must not be compromised by internal status events, such as self-exclusion orders and self-exclusion revocations.

3.3.11 Imposed Limitations

- a) The IGS must have a mechanism in place that permits the authorized operator to set limits on player accounts
- b) Players must be notified in advance of any authorized operator-imposed limits.

4.0.00 Software Requirements

4.1.01 General Statements

- a) With respect to the application of the RNG requirements listed in this document, it is accepted that predictability is not relevant to certain applications. SLGA, in conjunction with the testing laboratory, must determine whether predictability is relevant to the application being tested, and apply these requirements accordingly
- b) Any RNG outcomes used for game symbol selection/game outcome determination must be proven to:
 - i. Be statistically independent
 - ii. Be fairly distributed (within statistically expected bounds) over their range
 - iii. Pass various recognized statistical tests
 - iv. Be non-predictable
- c) Game symbol selection/game outcome determination must not be influenced, affected or controlled by anything other than numerical values or, where applicable, mechanical outcomes derived from the RNG in conjunction with the rules of the game. Note: this does not prohibit metamorphic games or Progressive Jackpots determined by means other than individual game outcomes from being considered on a case-by-case basis
- d) As game symbols are selected/game outcomes are determined, they must be immediately used as directed by the rules of the game (i.e., they are not to be discarded due to adaptive behavior by the game)
- e) Where the rules of the game require a sequence of game symbols/game outcomes to be set up in advance, these entities must not be re-sequenced except as provided by the rules.

4.1.02 Choice of RNG

The RNG can either be software-based, hardware-based, a combination of both, or a mechanical-based RNG, at the discretion of the authorized operator. However, the final implementation must comply with the requirements of this document.

4.1.03 Hardware-Based RNGs

Hardware-based RNGs can potentially ‘break down’ over time. Failure of a hardware-based RNG could have serious consequences for the IGS, as games may become predictable or exhibit non-fair distribution. If a hardware-based RNG is used, some form of dynamic/active, real-time monitoring of the output is required, such that game play is disabled in the event that a failure is detected.

4.1.04 Software-Based RNGs

The following requirements apply only to software-based RNGs.

4.1.05 Scaling

- a) The methods of scaling (i.e., converting raw RNG outcomes of a greater range into scaled RNG outcomes of a lesser range) must be linear, and must not introduce any bias, pattern or predictability
- b) The scaled RNG outcomes must be proven to pass various recognized statistical tests.

4.1.06 Period

The period of the RNG, in conjunction with the methods of implementing the RNG outcomes, must be sufficiently large to ensure that all game outcome combinations are possible for the given games/applications.

4.1.07 Range

The range of raw values produced by the RNG must be sufficiently large to provide adequate precision and flexibility when scaling and mapping.

4.1.08 Seeding/Re-Seeding

- a) The methods of seeding/re-seeding implemented in the RNG must ensure that all seed values are determined securely, and that the resultant sequence of game outcomes is not predictable
- b) Unless proven to have no adverse effect on the randomness of the RNG outcomes, seeding and reseeding must be kept to an absolute minimum
- c) If for any reason the background cycling/activity of the RNG is interrupted, the next seed value for the RNG must be a function of the value produced by the RNG immediately prior to the interruption.

4.1.09 Background Cycling/Activity

- a) In order to ensure that RNG outcomes cannot be predicted, adequate background cycling/activity must be implemented in between games
- b) Wherever a game outcome is made up of multiple mapped RNG values, background cycling/activity must be implemented during the game (i.e., in between the selection of each mapped RNG value) in order to ensure that the game outcome is not comprised of sequential mapped RNG outcomes
- c) The rate of background cycling/activity must be sufficiently random in and of itself to prevent prediction.

4.1.10 Unpredictability

The state of the RNG must be modified between every game unless a “cryptographic RNG” is implemented. If necessary to ensure unpredictability, such modification may be additionally required within a game. Note that hardware devices are considered to modify their state continuously. Possible modifications of RNG state that may satisfy this requirement include, but are not limited to:

- a) The discard of an unpredictable number of RNG values (i.e., background cycling). If the number of discarded values is determined by an RNG, it may not be determined by the primary RNG itself, but must instead be determined by a secondary RNG, independent and asynchronous to the primary RNG
- b) The overwriting (re-seeding) or mixing (entropy injection) of all or a portion of the RNG state by an external event or entropy source. The re-seeding or mixing shall be done in such a way that does not compromise the intended distribution, independence, or availability of prizes. The external event or entropy source shall not be able to be predicted or estimated by a player.

4.1.11 Cryptographic RNG

The use of a cryptographic RNG may not be feasible for every circumstance requiring an RNG, but shall be utilized where possible, as a cryptographic RNG is one that cannot be easily compromised by a skilled attacker with knowledge of the source code.

4.2.00 Game Behavior Requirements

4.2.01 Game Fairness

Games must be designed according to, but not limited to the following criteria:

- a) Games must not be designed to give the player a false expectation of better odds by falsely representing any occurrence or event
- b) Near-miss games that are specifically designed to give the player the perception that they almost won the top prize with a frequency greater than that which would naturally occur given the game rules in order to induce the player to continue gaming, are not permitted
- c) Games that are designed to give the player the perception that they have control over the game due to player skill, when they actually do not (i.e., the game outcome is fully random), are not permitted. It is permitted for a game to be designed to give the player the perception that the outcome may be due to player luck, provided that the player has been informed in the game rules that their choices cannot actually influence the outcome of the game
- d) The following information must be available to the player:
 - i. Rules of the game and instructions of play
 - ii. The %RTP value
 - iii. Odds of winning, or odds/payouts
 - iv. Applicable fees or commissions
- e) Further to subsection (d) above, where end player devices utilize mobile technologies, it is permissible to present an abridged version of the above information accessible from directly within the game, and make available the full/complete version of the above information through another method, such as a link to the information website
- f) The rules of the game must not be deceitful or misleading
- g) The rules of the game must be accurate and correct
- h) Game rules must not be changed during a session. The authorized operator must have a policy and procedure in place to prevent a game rule from being changed during a session unless effective notification is given to player
- i) Game rules must not be changed between a player making a bet and the decision to credit or debit the players account for the bet
- j) Further to subsections (h) and (i) above, there is the possibility of the following with sports wagering:
 - i. Dynamic odds/payouts setting, or
 - ii. Rule changes to address circumstances within the sport/contest/match (e.g., disqualified winners, cancelled games, etc.)
- k) Games/wagers must operate and interact with the player strictly in accordance with the published rules
- l) All players must be no more or no less eligible to win the game than players using the land-based method. Note: Promotions may be implemented on either the online or the land-based method alone.

4.2.02 Game Play Duration

The minimum duration for a single game is to be 3 seconds.

4.2.03 No Adaptive Behavior by Games

A player who plays a game that is represented as being based on a random event must have an equally likely chance of obtaining any possible combination every time a game is played (except for that which is provided in the game rules). That is, it is unacceptable for the %RTP to be manipulated by the system or manual intervention to maintain a constant %RTP.

4.2.04 No Forced Game Play

- a) The player must not be forced to play a game just by selecting that game
- b) The IGS must detect and reject repeated “play” messages that arise from impatient players pressing “play” more than once while awaiting a response from the IGS.

4.2.05 Game Play Requirements

- a) The following information must be displayed on the game screen, or accessible via a link:
 - i. Game name
 - ii. Instructions (and restrictions) on game play or available wagers, in the case of wagering on future events, including a pay table for all prizes and special features
 - iii. Current account balance displayed in currency (as opposed to credits)
 - iv. Unit and total bet
- b) The following principles must be followed where games are provided in different language versions:
 - i. Each language version of the same game/wager must provide the same %RTPs or odds/payouts
 - ii. Each language version must be consistent with the game/wager instructions and restrictions for that version
 - iii. All game information must be provided in the language specified for that version
 - iv. The game instructions (and restrictions) must carry the same meaning across all language versions so that no one version is advantaged or disadvantaged.

4.2.06 Game Design

- a) All pay table variations of any given game offered on the IGS must comply with all applicable requirements herein, and must exhibit a %RTP not less than a minimum value as agreed to by SLGA and the authorized operator for that particular game type
- b) The %RTP for each game must be specified by the authorized operator in the game documentation
- c) Where a progressive prize is offered, the calculated %RTP must include such factors as the base game %RTP, progressive start-up value, progressive increment rate, etc.
- d) %RTP for a game must be demonstrable, as well as theoretical, and must be of a similar %RTP to those games typically found in traditional/land-based gaming venues/sites. Where a game does not have a traditional/land-based equivalent, SLGA reserves the right to withhold game approval if, in its judgment and having regard to all circumstances, the %RTP is not considered to be fair and reasonable
- e) Where a game is represented or implied to include a simulation of a real-life physical device, the behavior of the simulation must be identical to the expected behavior of the real-life physical device. That is:
 - i. The visual representation of the simulation must correspond to the features of the real-life physical device, insofar as it is material to ensuring player fairness and clarity
 - ii. The probability of any event occurring in the simulation that affects the outcome of

- the game must be equivalent to the real-life physical device
- iii. Where the game simulates multiple real-life physical devices that would normally be expected to be independent of one another, each simulation must be independent of the other simulations
- iv. Where the game simulates real-life physical devices that have no memory of previous events, the behavior of the simulations must be independent of (i.e., not correlated with) their previous behavior, so as to be non-adaptive and non-predictable in practice.

Note: The intent of item (e) above is not to limit options from a game design perspective, but rather to ensure that the player is not misled by the behavior of a simulation. For example, it is acceptable for a game to implement a roulette wheel that has only 12 numbers, instead of the traditional 37 or 38 numbers, provided that this behavior has been made clear to the player. In this instance, item (e) would apply in that the probabilities for the roulette wheel with 12 numbers must align with the real-life physical equivalent (i.e., a 1/12 chance of yielding any particular number).

- f) Games not completely independent of game play history (i.e., metamorphic games) must:
 - i. Display clearly to the player which game rules apply to the current game state
 - ii. Display to the player sufficient information to indicate the current status towards the triggering of the next metamorphosis of the game. If the game collects tokens, the number of tokens missing or the total number required to trigger the next metamorphosis must be indicated, along with the number of tokens collected at that point
 - iii. Not adjust the likelihood of a metamorphosis occurring based on the history of prizes obtained in previous games. Games must not adapt their %RTP based on past payouts
 - iv. Not be designed in such a manner to be misleading to the player.

4.2.07 Mapping

- a) The methods of mapping (i.e., converting scaled RNG outcomes into actual game symbols/game outcomes) must also be linear. Note: it is accepted that certain game implementations require exemption from this requirement, such as instances where mapping is purposefully used to create the necessary probabilities for various game outcomes, as provided by the rules of the game
- b) The mapped RNG outcomes must be proven to pass various recognized statistical tests.

4.2.08 Game Play

- a) Wagering that requires monetary payment (i.e., play-for-real) can only occur during a game session (i.e., after the player has logged in, and before the player has logged out)
- b) Where links are used to supply information as required by this Standard, game play must not occur if the linked information is not available. These links must be checked (either manually or automatically) at least daily.
 - i. Where a broken link is uncovered, and the link relates to game-specific information only, then the associated game(s) must be taken offline (either manually or automatically) if the link is not repaired within one hour
 - ii. Where a broken link is uncovered, and the link relates to the website as a whole, then all games must be taken offline (either manually or automatically) if the link is not repaired within twelve hours

- c) In the event that a game in current play cannot be continued due solely to an IGS action, all bets must be returned to the players of that game
- d) If the IGS extends an invitation to play a particular game, it must accept all legitimate wagers (as defined by rules) for that game
- e) At the time of selection, the player must be made aware of which game or wager is being selected for play
- f) It must not be possible to start a second occurrence of the same game before the current game in play is completed and all relevant meters have been updated on the IGS. Some exceptions may be granted in instances where, for example:
 - i. the authorized operator elects to issue a manual process for large payouts (e.g., where a player chooses to continue gaming while a payout is pending)
 - ii. The game in question is based on a future event, such as with sports wagering or a periodic lottery drawing
- g) A ‘replay last game’ facility must be provided, either as a re-enactment or by description. The replay must clearly indicate that it is a replay of the previous game, and must provide the following information (at a minimum):
 - i. The date and time the game was played
 - ii. The display associated with the final outcome of the game, either graphically or via a clear text message
 - iii. Total player cash/credits at start of play
 - iv. Total player cash/credits at end of play
 - v. Amount bet including any multipliers
 - vi. Total cash/credits won for the prize resulting from the last play
 - vii. The results of any player choices involved in the game outcome
 - viii. Results of any intermediate game phases, such as gambles or feature games
- h) For games that involve wagering on a future event, such as with sports wagering or a periodic lottery drawing, a ‘Wager History’ must instead be provided. The history must clearly indicate that it is a history of the previous wager(s), and must provide the following information (at a minimum):
 - i. The date and time the wager was placed
 - ii. The description of the final outcome of the game upon which the wager was made, either graphically or via a clear text message
 - iii. Total player cash/credits upon placing the wager
 - iv. Total player cash/credits upon settlement of the wager
 - v. Amount wagered including any multipliers
 - vi. Total cash/credits won for the wager (including Progressive Jackpots)
 - vii. Any player choices involved in the wager
 - viii. Results of any intermediate wager phases.

4.2.09 Game Artwork (Information Displayed)

This section refers to all relevant graphical and auditory information being presented to the player and must comply with these requirements.

4.2.10 Instructions and Information

- a) All information presented on the gaming platform must comply with applicable content, advertising and marketing rules for Saskatchewan
- b) All written information presented on the gaming platform and games must be available in English (Note: logos or copyright messages may be displayed). This does not preclude the display of the same information in other languages
- c) All written information presented on the gaming platform and games must be truthful and correct
- d) All game help/rules information (or wagering instructions, in the case of wagering on future events, such as sports) must be clearly visible, or the means of displaying such information must be readily available at all times
- e) All game help/rules information (or wagering instructions, in the case of wagering on future events such as sports) must be visible/available to the player without the need for money to be bet on the game
- f) All game help/rules information (or wagering instructions, in the case of wagering on future events such as sports) must be accurate and correct
- g) There must be sufficient game help/rules information to allow a player to determine the correctness of the game or wager outcome
- h) If random prizes are offered, the maximum value obtainable from the random prize must be indicated in the game help/rules information
- i) If the value of the random prize depends on the amount of money wagered, this must also be stated in the game help/rules information
- j) For non-event based games, a pay table displayed in the game artwork must correspond to the pay table used in the mathematical treatise, and correspond to the pay table implemented in the actual game design
- k) The functions of all buttons represented must be clearly indicated:
 - i. Where possible on the button
 - ii. On the help/rules screen
- l) The rules of the game, as made available to the player using the internet interface/gateway, must include the same information as that which is made available to the player using the land-based method
- m) The artwork and functionality of the game, as made available to the player using the internet interface/gateway, must not result in any advantage or disadvantage as compared with the player using the land-based method

4.2.11 Bet Display

- a) The bet denomination (and, where applicable, the tokenization) of the game must be clearly visible on the game screen or be able to be easily deduced
- b) All selections in a wager must be displayed to the player
- c) If a game uses tokenization, the number of credits registered for each monetary unit for the current game must be displayed on the game screen
- d) The artwork must either state the maximum bet, the number of credits that can be bet per selected line and the number of possible lines available, or it must be possible to deduce this information from the game help/rules
- e) The minimum bet (if not easily deduced) must be readily available to the player, either directly on the game screen or in the game help/rules information.

4.2.12 Result Display

- a) The display of the result of a game's final outcome must not be misleading or deceptive to the player
- b) The final outcome of each game must be displayed for a sufficient length of time that permits a player to verify the outcome of the game
- c) The display of the results of a wager based on a future event must be made available through the player's wager history facility
- d) The nature of all prizes must be clearly indicated. If some prizes are in cash, with others are in credits, this must be stated
- e) If the artwork contains game instructions specifying a maximum win, then it must be possible to win this amount from a single game (including features or other game options)
- f) To the extent that is practicable for the range of games offered, only one method of displaying win amounts will be used on the website so as to avoid confusion

4.2.13 Game-Specific Requirements

All gaming devices and associated gaming components approved for use in Saskatchewan must be certified in accordance with SLGA standards, policies and regulations. Where an SLGA standard does not exist, SLGA:

- a) Refers directly to applicable GLI technical standards
- b) Reserves the right to impose technical requirements consistent with regulation.

5.0.00 Player Location Requirements

5.1.01 General Statements

The requirements within this section shall apply for player location detection.

5.1.02 Fraud Prevention

The IGS shall incorporate the best practices and security measures to limit risk related to:

- a) Location data fraud (e.g., fake location apps, virtual machines, remote desktop programs, etc.)
- b) System-level tampering (e.g., rooting, jailbreaking, etc.)
- c) "Man-In-The-Middle" attacks or similar hacking techniques
- d) Emerging location fraud risks

5.1.03 Detection on a Private Network

Where interactive gaming occurs over a private network, such as a Wireless Local Area Network (WLAN), the IGS must incorporate methods that can track the locations of all players connected to the network.

5.1.04 Detection on a Public Network

Where interactive gaming occurs over a public network, such as the internet, the IGS shall incorporate a location detection service or application to reasonably detect and dynamically monitor the location of a player attempting to play a game, and to monitor and enable the blocking of unauthorized attempts to play a game.

6.0.00 Progressive Jackpots

6.1.00 Progressive Jackpot Game Requirements

6.1.01 General Statements

A game is deemed to include a Progressive Jackpot component when the game has an integrated or stand-alone incremental prize that increases based on a function of credits that are wagered. This includes games that award Progressive Jackpots or a “pool” based on criteria other than obtaining winning symbols, such as mystery jackpots, bad-beat jackpots etc. Incremental prize jackpots roll over into the next game if they are not won in the current game.

6.1.02 Progressive Jackpot Fairness

- a) All players that play games or place wagers that implement some form of Progressive Jackpot must be made aware of how they can be eligible to win the Progressive Jackpot
- b) The rules of the game/wager must include how the Progressive Jackpot is funded and determined
- c) All players contributing to the Progressive Jackpot and meeting all other eligibility requirements according to the game rules, must be eligible to win the Progressive Jackpot while they are playing that game (or having placed a wager on that game, in the case of wagering on future events such as sports)
- d) Progressive Jackpot contributions must not be assimilated into revenue. For example, if a cap is established on any Progressive Jackpot, all additional contributions once that cap is reached must be credited to a Diversion Pool
- e) If a minimum bet amount exists in order for a player to win a jackpot, then the base game must meet the minimum %RTP value.

6.1.03 Notification of the Progressive Jackpot Amount

- a) The current Progressive Jackpot amount must be displayed on all end player devices participating in the Progressive Jackpot
- b) It is acceptable that the system display to the player, a minimum figure for the Progressive Jackpot amount, instead of the current exact figure, provided that:
 - i. Under no circumstances is the actual Progressive Jackpot amount less than the minimum figure displayed to the player
 - ii. It is made clear to the player that the displayed figure is a minimum value
 - iii. The actual Progressive Jackpot amount is displayed to all participating players at the time of the Progressive Jackpot being won (or earlier)
- c) End player device displays at least every 30 seconds. Internet communication delays may be beyond the control of authorized operator, so server-to-client delays may occur
- d) Players must be notified in the terms and conditions of game play and of the imperfections of internet communications.

6.1.04 Progressive Jackpot Win Notification

Players must be notified of the win (including the amount won) by the end of their game in play.

6.1.05 Progressive Jackpot Parameter Changes

Once a Progressive Jackpot has commenced, parameter changes must not take effect immediately. These parameter changes must instead be saved to apply after the current Progressive Jackpot is won.

6.1.06 Multiple Progressive Jackpot Winners

The authorized operator must address the possibility of a Progressive Jackpot being won (or appearing to be won) by one or more players at approximately the same time. The rules of the game must include resolution of this possibility.

6.1.07 Conversion of Progressive Jackpots

The authorized operator must have a policy and procedure in place to convert or combine one Progressive Jackpot pool into another Progressive Jackpot pool.

6.1.08 Progressive Jackpot Financial Liability

The rules of the game must provide for any planned or unplanned termination/discontinuation of a Progressive Jackpot. Of particular concern is how any outstanding pool amounts are dealt with in order to ensure player fairness.

6.1.09 Progressive Jackpot Shutdown

There are instances in this document where it is indicated that the Progressive Jackpot must be “shutdown”. A Progressive Jackpot shutdown requires the following action:

- a) Clear indication must be given to players that the Progressive Jackpot is not operating by displaying a message such as “Jackpot Closed” on end player devices
- b) It must not be possible for the Progressive Jackpot to be won while in the shutdown state
- c) Activation of the Progressive Jackpot from the shutdown state must reinstate the Progressive Jackpot with the identical parameters (including Progressive Jackpot value, and hidden win amount for Mystery Progressive Jackpot) as before the shutdown.

6.1.10 Progressive Jackpot Meters

For internal authorized operator use, the IGS must store and maintain the following software meters at a minimum:

- a) Total amount contributed/won (normally equal) for each previous Progressive Jackpot, including separate figures for any diverted amounts
- b) Grand total amount contributed/won (normally equal) for all previous Progressive Jackpot combined
- c) Total amount contributed for the current Progressive Jackpot, including separate figures for any diverted amounts.

6.1.11 Progressive Jackpot Recovery

In order to enable the recovery of the current value of the Progressive Jackpot amount in the case of an IGS failure, either:

- a) The current value of the Progressive Jackpot amount must be stored in at least two physically separate devices, or
- b) The current value of the Progressive Jackpot amount must be able to be accurately calculated from other available metering information that is not stored in the same system as the Progressive Jackpot amount.

6.1.12 Progressive Jackpot Controller

The Progressive Jackpot controller is deemed to be part of the IGS, even if it is a physically separate controller. Where a “Master Controller” employs “Slave Controllers” to control a Progressive Jackpot, the following requirements apply:

- a) All Slave Controllers must be time synchronized with the Master Controller
- b) The Master Controller must be time synchronized with the IGS
- c) Game result Progressive Jackpot win events must be time stamped and the Progressive Jackpot Controller must ensure that hits registered within a minimum time increment are considered as simultaneous wins. The minimum time window (Progressive Jackpot Reset Period) is not less than the longest time taken to:
 - i. Register that a Progressive Jackpot has been won
 - ii. Announce the win on the displays of all participating end player devices, and
 - iii. Reset the Progressive Jackpot meters.

7.0.00 Integrity of the Gaming System

7.1.01 Monitoring

To maintain security and integrity, and in order to remain in compliance with prevailing regulation, the IGS must be diligently monitored. This includes assessing the website and its control environment, on an ongoing basis, fraud, risk, relevant updates, fixes, or software changes.

7.1.02 Change Management

There must be a process implemented 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 channel 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) For any required testing, the type of testing and timing for that testing must be identified
- 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.

Definitions

Critical Functions

Behaviors and functions relative to the integrity of gaming as defined by SLGA. This includes, but is not limited to, encryption, auditability, redundancy, and protection of assets and personal information.

Firewall

A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between an internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

Gaming Session

The period of time commencing when a player initiates a game or series of games by committing a wager and ending at the time of a final game outcome for that game or series of games and coincident with the opportunity for the player to retrieve their credit balance

Global System for Mobile Communications (GSM)

A standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation (2G) digital cellular networks used by mobile devices.

Hypertext transfer protocol secure (HTTPS)

A secure version of HTTP, which is the primary protocol used to send data between a web browser and a website. HTTPS is encrypted in order to increase security of data transfer. This is particularly important when users transmit sensitive data, such as by logging into a bank account.

ISO/IEC 27001

These standards were published by the International Organization for Standardization and the International Electrotechnical Commission (IEC) as a broad set of best practices for managing information security. ISO 27001 is a security standard that requires an information security management system (ISMS) be used to ensure an organization's security controls adequately address the organization's security needs and vulnerabilities.

Link Utilization

Link utilization is the ratio of the time that the link is active to the total time. Total time being the sum of transmission time and propagation time.

Man-In-The-Middle

A man-in-the-middle attack is like eavesdropping. When data is sent between a computer and a server, a cybercriminal can get in between and spy. A man-in-the-middle attack requires three players: the victim, the entity with which the victim is trying to communicate, and the "man in the middle" intercepting the victim's communications.

Multi-Factor Authentication

A type of authentication which uses two or more methods to verify a user's identity. This includes a variety of possible techniques, but generally involve information known only to the user and an item possessed by a user (e.g., an electronic token or value on an alternative device). In some cases, a user's biometric data (e.g., fingerprints, facial or voice recognition) can also be used.

Open Source Security Testing Methodology Manual (OSSTMM)

The Open Source Security Testing Methodology Manual, or OSSTMM, is a peer-reviewed methodology for security testing, maintained by the Institute for Security and Open Methodologies (ISECOM).

Percentage Return to Player (%RTP)

A ratio of the ‘total amount won’ to the ‘total amount wagered’ by a player. Such a return may be “theoretical” (based on mathematical calculations or simulations) or “actual” (based on the metering supported by a fielded gaming device). The minimum legislated %RTP in Saskatchewan is 85% for slots and 90% for video lottery terminals.

Progressive Jackpots (for Systems and Games)

A system that takes contributions from one or more gaming devices and applies it to an incrementing award. When the proper condition or trigger occurs, the award is paid to a player.

Proxy Service

A proxy server is essentially a computer on the internet that has an IP address of its own. Proxies provide a valuable layer of security for your computer. They can be set up as web filters or firewalls, protecting your computer from internet threats like malware.

Random Number Generator (RNG)

A computational or physical device, algorithm, or system designed to produce numbers in a manner indistinguishable from random selection.

Rootkits

A set of software tools that enable an unauthorized user to gain control of a computer system without being detected.

Scaling

An algorithm or method by which the numbers selected by an RNG are scaled or mapped from a greater range to a lesser range for use in the game.

Virtualization

Virtualization is when a simulated computing environment is created instead of a physical version. Computer hardware and operating systems can be virtualized.

Virtual Private Network

A method employing encryption to provide secure access to a remote computer over the internet.

Wireless Local Area Network

A wireless local area network (WLAN) is a wireless distribution method for two or more devices that use high-frequency radio waves and often include an access point to the Internet.