STANDARD SERIES

GLI-19:

Interactive Gaming Systems

(Operators)

Version: 1.0

Release Date: 31 May 2011

Copyright © 2011 GLI Interactive BV All Rights Reserved.

This Page Intentionally Left Blank

Copyright © 2011 GLI Interactive BV All Rights Reserved.

ABOUT THIS STANDARD

This Standard has been produced by **TST, A GLI Company** for the purpose of providing independent certifications to suppliers under this Standard and complies with the requirements set forth herein.

An operator should submit equipment with a request that it be certified in accordance with this Standard. Upon certification, TST, A GLI Company will provide a certificate of compliance evidencing the certification to this Standard.

Copyright © 2011 GLI Interactive BV All Rights Reserved.

Table of Contents

CHAPTER 1 6

1.0 Overview – Standards for Interactive Gaming Systems 6
1.1 Introduction 6
1.2 Acknowledgment of Other Standards Reviewed 7
1.3 Purpose of Technical Standards 8
1.4 Interpretation of this Document 8
1.5 Other Documents That May Apply 9

CHAPTER 2 10

2.0 Gaming Platform Requirements 10
2.1 Reserved 10
2.2 Gaming Platform 10
2.3 Gambling Information to be Maintained by the Gaming Platform 12

CHAPTER 3 16

3.0 Player Account Management Requirements 16
3.1 Player Registration 16
3.2 Player Accounts 17
3.3 Player Game Session 19
3.4 Player Loyalty Programs 20
3.5 Responsible Gaming 20

CHAPTER 4 25

4.0 Reserved 25

CHAPTER 5 26

5.0 Game Requirement 26
5.1 Game Design 26
5.2 Game Artwork 27
5.3 Peer to Peer (P2P) Games 28
5.4 Game Play 29

CHAPTER 6 33

6.0 Jackpot (Progressive) Requirements 33
6.1 Introduction 33
6.2 Jackpot Design and Operation 33

CHAPTER 7 38

7.0 Information Systems Security (ISS) Requirements 38
7.1 General Statement 38
7.2 Information Security Policy 38
7.3 Physical and Environmental Controls 39
7.4 Administrative Controls 40
7.5 Technical Controls 43

Glossary 52

Copyright © 2011 GLI Interactive BV All Rights Reserved.

Appendix A: Submission Requirements 56

A.1 Introduction 56
A.2 Prototype (Full Submission) Submissions 56
A.3 Submissions of Modifications (Partial Submissions) to a Previously Certified Item 62

Copyright © 2011 GLI Interactive BV All Rights Reserved.

CHAPTER 1

1.0 Overview – Standards for Interactive Gaming Systems

1.1 Introduction

1.1.1. General Statement. In recent years, many jurisdictions have opted to ask for standards tests without creating their own standards documents. In addition, with technology changing almost monthly, new technology is not being incorporated quickly enough into existing standards due to the long process of administrative rulemaking. This document, *GLI Standard 19*, will set forth the technical Standards for Interactive Gaming Systems used in an Internet environment.

1.1.2 Document History. We have listed below, and give credit to, agencies whose documents we reviewed prior to writing this Standard. It is the policy of **TST, A GLI Company** to update this document as often as possible to reflect changes in technology, testing methods, or cheating methods.

This document will be distributed FREE OF CHARGE to all those who request it. It may be obtained by downloading it from our websites at www.gaminglabs.com, www.tstglobal.com or by emailing us at: **compliance@gaminglabs.com**

Copyright © 2011 GLI Interactive BV All Rights Reserved.

1.2 Acknowledgment of Other Standards Reviewed

1.2.1 General Statement. These Standards have been developed by reviewing and using portions of the documents from the organizations listed below. We acknowledge the regulators who have assembled these documents and thank them:

a) The ACT Office of Financial Management;
b) The Alderney Gambling Control Commission;
c) The Antigua & Barbuda Financial Services Regulatory Commission;
d) The British Columbia Gaming Policy and Enforcement Branch;
e) The Italy Autonomous Administration of State Monopolies;
f) The New South Wales Department of Gaming and Racing;
g) The Northern Territory Racing and Gaming Authority;
h) The New Zealand Casino Control Authority;
i) The New Zealand Department of Internal Affairs, Gaming Racing & Censorship Division;
j) The Queensland Office of Gaming Regulation;
k) The South African Bureau of Standards;
l) The South Australian Office of the Liquor and Gaming Commissioner;
m) The Tasmanian Department of Treasury and Finance, Revenue and Gaming Division;
n) The United Kingdom Gambling Commission;
o) The Victorian Casino and Gaming Authority;
p) The Western Australian Office of Racing Gaming and Liquor.

Copyright © 2011 GLI Interactive BV All Rights Reserved.

1.3 Purpose of Technical Standards

1.3.1 ***General Statement***. The Purpose of this Technical Standard is as follows:

a) To eliminate subjective criteria in analyzing and certifying Interactive Gaming System (IGS) operation.

b) To only test those criteria which impact the credibility and integrity of Interactive Gaming Systems from both the revenue collection and player's point of view.

c) To create a standard which will ensure that games made available via the Internet are fair, secure, and able to be audited and operated correctly.

d) To distinguish between local public policy and laboratory criteria. At TST, A GLI Company we believe that it is up to each local jurisdiction to set its own public policy with respect to gaming.

e) To recognize that the evaluation of internal control systems (such as Anti-Money Laundering, Financial and Business processes) employed by the operators of the Interactive Gaming System should not be incorporated into this standard but left to the Regulatory Body of each local jurisdiction to assess as part of the licensing process.

f) To recognize that non-gaming testing (such as Electrical Testing) should not be incorporated into this standard but left to appropriate test laboratories which specialize in that type of testing. Except where specifically identified in the standard, testing is not directed at health or safety matters. These matters are the responsibility of the manufacturer, purchaser, and operator of the equipment.

g) To construct a standard which can be easily changed or modified to allow for new technology.

h) To construct a standard which does not specify any particular method or technology for any element or component of an Interactive Gaming System. The intent is to allow a wide range of methods to be used to conform to the standards, while at the same time encouraging new methods to be developed.

1.4 Interpretation of this Document

1.4.1 ***No Limitation of Technology***. One should be cautioned that this document should

Copyright © 2011 GLI Interactive BV All Rights Reserved.

not be read in such a way that limits the use of future technology. The document should not be interpreted that if the technology is not mentioned, then it is not allowed. Quite to the contrary, as new technology is developed, we will review this standard, make changes and incorporate new minimum standards for the new technology.

1.4.2 Software Suppliers and Operators. The components of an Interactive gaming System, although they may be constructed in a modular fashion, are designed to work seamlessly together. In addition, Interactive Gaming System components may be developed to have configurable features, the final configuration of which will depend on the options chosen by the end operator. From a testing perspective, it may not be possible to test all of the configurable features of an Interactive Gaming System component submitted by a software supplier in the absence of the final configuration chosen by the operator.

This document has been designed to focus on operator specific test requirement. Because of the integrated nature of an Interactive Gaming Systems there are a number of requirements in this document which may apply to both operators and suppliers. In these cases, where testing is requested for a "white-label" version of the component, a specific configuration will be tested and reported.

This document is not intended to be arbitrary in defining which parties are responsible for meeting the requirements of this document. It is left to the stakeholders of each system to determine how best to meet the requirements laid out in this document.

1.5 Other Documents That May Apply

1.5.1 General Statement. This standard covers the actual requirements for single-player and multi-player games being played through the use of various devices such as personal computers and mobile devices via the Internet. Currently there are no other documents, which may apply.

Copyright © 2011 GLI Interactive BV All Rights Reserved.

CHAPTER 2

2.0 Gaming Platform Requirements

2.1 Reserved

2.2 Gaming Platform

2.2.1 ***General Statement***. If the Gaming Platform is comprised of multiple computer systems at various sites, the Gaming Platform as a whole and all communication between its components must conform to these requirements.

2.2.2 ***Shut Down and Recovery***. The Gaming Platform must have the following shutdown and recovery capabilities:

a) The Gaming Platform must be able to recover from unexpected restarts of its central computers or any of its other components;
b) The Gaming Platform must be able to perform a graceful shut down in the event of a simple power failure, and only allow automatic restart on power up after the following procedures have been performed as a minimum requirement:
    i) Program resumption routine(s), including self tests, complete successfully;
    ii) All critical files of the Gaming Platform have been authenticated using an approved method (ex. CRC, MD5, SHA-1, etc); and
    iii) Communication with all components necessary for Gaming Platform operation have been established and similarly authenticated.
c) The Gaming Platform must be able to identify and properly handle the situation where master resets have occurred on other Gaming Platforms which affect game outcome, win amount or metering;
d) The Gaming Platform must be able to recover all critical information from the time of the last backup to the point in time at which the Gaming Platform failure or reset occurred (no time limit is specified);

Copyright © 2011 GLI Interactive BV All Rights Reserved.

e) The system must have the capability sufficient to ensure that player entitlements and audit-ability is available at all times.

2.2.3 Third Party Hosting. Where one or more components of the Gaming Platform are hosted by a third party service provider, the following requirements must be met:

a) The private and financial information of all players must not be accessible by the third-party service however; this does not preclude the use of third party services for backup and data storage;

b) Any gaming functionality must not be accessible by the third-party service;

c) No third party service may be used which requires software to comply with rules/regulations which are contradictory to any items found within this document.

2.2.4 Disabling of Gambling. The following requirements apply to the disabling and enabling of gambling on the Gaming Platform:

a) The Gaming Platform must be able to disable or enable all gambling on command;

b) The Gaming Platform must be able to disable or enable individual games on command;

c) The Gaming Platform must be able to disable or enable individual player sessions on command; and

d) When any gambling is disabled or enabled on the Gaming Platform an entry must be made in the audit log. The reason for any disable must be recorded in a protected audit log which does not necessarily have to be part of the Gaming Platform.

2.2.5 User Inactivity Timeout. If the Gaming Platform is not capable of polling the end player device to confirm a connection, it should implement user inactivity timeouts.

2.2.6 Polling of End Player Devices. If the Gaming Platform is capable of polling, it must be able to poll end player devices on a time schedule basis and on command from a Gaming Platform operator, and:

a) The Gaming Platform must be able to store the time and date of the last poll that occurred;

Copyright © 2011 GLI Interactive BV All Rights Reserved

b) Failure of an end player device to respond within 30 minutes must cause the session to be terminated; and
c) The end player device must assume session termination if it fails to receive a response from the server within 30 minutes. The end player device must notify the player of session termination. No further game play is permitted until the Gaming Platform and the end player device establish a new session.

2.2.7 Malfunction. The Gaming Platform must:

a) Not be affected by the malfunction of end player devices other than to institute the incomplete games procedures in accordance with these requirements; and
b) Include a mechanism to void bets and pays in the event of a malfunction of the Gaming Platform itself if a full recovery is not possible.

2.3 Gambling Information to be Maintained by the Gaming Platform

2.3.1 General Statement. The operator must retain gambling information for a period of seven years from the current point in time. This information may be stored offline. All time stamping must be in a single time, and if the time chosen is not Coordinated Universal Time (UTC) then the difference to UTC must be apparent.

2.3.2 Player Account Information. For each player account the information to be maintained, backed up and be available for inclusion in reports by the Gaming Platform must include:

a) Player identity details (including verification method);
b) Player agreement to the operator's Terms and Conditions and Privacy Policy;
c) Account details and current balance;
d) Maximum bet loss levels, and exclusion status;
e) Previous accounts and reason for de-activation; and
f) The current session information.

2.3.3 Session Information. For each gaming session (i.e.: customer login time to logout time), the information to be maintained, backed up and be available for inclusion in reports by the Gaming Platform must include:

a) Unique player ID;

Copyright © 2011 GLI Interactive BV All Rights Reserved

b) Session start and end time;
c) Relevant player device details such as IP address and browser and/or client version;
d) Total monies wagered for session;
e) Total monies won for session;
f) Funds added to account for session (time-stamped);
g) Funds withdrawn from account for session (time-stamped);
h) Where polling is implemented, time of last successful poll for session;
i) Reason for session termination;
j) Where polling is implemented, game play information for session; (i.e. games played, amounts bet, amounts won, jackpots won etc.);
k) Player account balance at the start of the session;
l) Current active sessions (e.g.: in progress, complete, etc.); and
m) Time and date of interruption.

2.3.4 Game Play Information. For each individual game played the information to be maintained, backed up and be available for inclusion in reports by the Gaming Platform must include:

a) Unique player ID;
b) Game start time according to the Gaming Platform;
c) Account balance at start of game;
d) Wager for game;
e) Contributions to Jackpot pools (if applicable);
f) Game status (in progress, complete, etc);
g) Game result and outcome;
h) Jackpot win (if applicable);
i) Game end time according to the Gaming Platform;
j) Amount won;
k) Account balance at the end of the game;
l) The table number (if applicable) at which the game is played;
m) The paytable used; and
n) Game identifier and version.

Copyright © 2011 GLI Interactive BV All Rights Reserved

2.3.5 Jackpot Information. The jackpot meter information must be transferred from the Jackpot Controller to the Gaming Platform at least every 60 seconds. At a minimum, the following jackpot software meters must be maintained, backed up and be available for inclusion in reports by the Gaming Platform:

a) Total amount played for jackpots;
b) Total amount of jackpots won;
c) Total jackpot contributions made, (includes any diverted amounts);
d) Total jackpot contributions won;
e) Jackpot start up or other seeds which are not funded from contribution;
f) Current amount for each jackpot; and
g) Current value of Jackpot contributions diverted.

2.3.6 Significant Event Information. The following requirements apply to the logging of significant event information by the Gaming Platform:

a) Significant event information to be maintained, backed up and be available for inclusion in reports by the Gaming Platform must include:
    i) Large wins in excess of the value specified by the licensing jurisdiction;
    ii) Large transfers of funds (single and aggregate over defined time period) in excess of the value specified by the licensing jurisdiction;
    iii) Changes made by the operator to game parameters;
    iv) Changes made by the operator to jackpot parameters;
    v) New jackpots created;
    vi) Jackpot win occurrences;
    vii) Jackpots retired;
    viii) Player exclusions (including reason for exclusion, requests to lift exclusion, and actual lifting of exclusion);
    ix) Events occurring in external Gaming Platforms which affect game outcome and win amounts (e.g. external jackpot hosts);
    x) Irrecoverable loss of customer-related data; and
    xi) Significant periods of Gaming Platform unavailability.

Copyright © 2011 GLI Interactive BV All Rights Reserved

b) External Gaming Platforms which affect game outcome or win amounts must maintain a log of significant events if they are not transferred immediately to the Gaming Platform;
c) The Gaming Platform must be able to receive and store all significant events from external Gaming Platforms which affect game outcome or win amounts;
d) The Gaming Platform must be able to provide a means to view significant events including the ability to search for particular event types; and
e) The Gaming Platform must be able to prioritize events based on their significance (e,g, whether to log an event, raise an alarm or disable gaming).

2.3.7 ***Result Recall Mechanism***. The following records must be maintained by the Gaming Platform to facilitate the recovery of incomplete games:

a) The Gaming Platform must maintain records of any game that fails to complete and the reason why the game failed to complete. This information is to be treated as vital information to be recovered by the Gaming Platform in the event of a failure.
b) Information sufficient to continue a partially complete game must be retained by the Gaming Platform. This information is to be treated as vital information to be recovered by the Gaming Platform in the event of a failure.
c) Bets associated with a partially complete game that can be continued must be held in a separate register until the game completes. Player accounts must reflect any funds held in the incomplete game register.
d) In the event that a game cannot be continued due to a Gaming Platform action, all bets must be returned to the players of that game.

2.3.8 ***Data Backup***. There must be a method to back up all critical data (which comprises financial, security and event information) with sufficient frequency to allow recovery in the event of an interruption.

Copyright © 2011 GLI Interactive BV All Rights Reserved

CHAPTER 3

3.0 Player Account Management Requirements

3.1 Player Registration

3.1.1 ***General Statement***. This section discusses the principles which apply to the creation, use, security and privacy of player registration details. The player registration information must be maintained on a secure part of the Gaming Platform and meet the following rules:

a) The player must be registered with the operator before any gambling can occur. However, it is acceptable for player to play for fun without registering;

b) If registration is performed on-line, the system must require entry of information to verify proof of identity, age, place of residence and acceptance of the Terms and Conditions set out by the regulator of the jurisdiction in which the gaming occurs;

c) If the system processes any part of the registration on-line, the system must ensure that access to the information is restricted to the person supplying the information and to authorized staff of the operator;

d) If the system processes any part of the registration off-line, the system must not permit a player to commence playing for money, but may permit "play for fun" activities, until the registration process is authenticated through some other communication described in the approved control system of the operator;

e) During the registration process, the player must agree to the operator's Terms and Conditions of service and the operator's Privacy Policy;

f) Once registered by an operator, each player must have a unique identifier, to enable identification of the appropriate player and account details by system each time a player commences a session;

g) Any initial password must be issued securely to the player;

h) The player must be advised to keep their password and login ID secure;

i) The player must be informed of what mechanisms exist to detect if there is unauthorised use of their account, such as observing the Last Log in Time Display, the IP address of

Copyright © 2011 GLI Interactive BV All Rights Reserved.

the last log in and reviewing credit card statements against known deposits;

j) A full identity check must be undertaken each time an individual attempts to register, with player authentication to be performed at the commencement of each game session;
k) Details of player verification must be kept on-line in a secure manner; and
l) A list of all player registrations (current or otherwise) and accounts (active or otherwise) must be maintained on-line.

3.2 Player Accounts

3.2.1 General Statement. The following rules apply to player accounts, which must be maintained on a secure part of the Gaming Platform.

a) Only players of the legal gambling age for the jurisdiction may be registered.
b) Funds from a player account may only be used for betting if the player is registered with the operator;
c) The Gaming Platform must not accept a bet that would cause a player's account to become negative;
d) A person who is excluded from game play must not be able to establish a new account. However, operators must be able to return the balance of the player's account subject to there being no other claims on the account; and
e) Where an account is terminated, all player accounts established as a result of that must be de-activated and the current balances returned to the players.

3.2.2 Establishment of Player Accounts. A new account for a person must not be created if the reason for the de-activation of a player registration associated with previous accounts indicates that the person must not be permitted to establish another account.

3.2.3 Privacy of Player Information. Any information obtained by operators in respect to player registration or account establishment must not breach the operator's Privacy Policy. In addition, the following rules shall be met:

a) Any information about the current state of player accounts must be kept confidential by the operator, except where the release of that information is required by law;

Copyright © 2011 GLI Interactive BV All Rights Reserved.

b) All player information must be securely erased (i.e. not just deleted) from hard disks, magnetic tapes, solid state memory and other devices before the device is decommissioned. If erasure is not possible, the storage device must be destroyed.

3.2.4 Player Funds Maintenance. The following principles must apply to the maintenance of player funds:

a) Player accounts on the Gaming Platform must be secured against invalid access or update other than by approved methods;
b) All deposit, withdrawal, transfer or adjustment transactions are to be maintained in a Gaming Platform audit log;
c) A deposit into a player's account made via a credit card transaction or other methods which can produce a sufficient audit trail must not be available for betting until such time as the funds are received from the issuer or the issuer provides an authorization number to the operator indicating that the funds are authorized. The authorization number is to be maintained in an Gaming Platform audit log;
d) Positive player identification, including any Personal Identification Number (PIN) entry or other approved secure methods, must be completed before the withdrawal of any monies held by the Gaming Platform can be made;
e) Inactive accounts holding monies in the Gaming Platform must be protected against illicit access or removal;
f) All transactions involving monies are to be treated as vital information to be recovered by the Gaming Platform in the event of a failure;
g) Payments from an account are to be paid (including funds transfer) directly to an account with a financial institution in the name of the player or made payable to the player and forwarded to the player's address. The name and address are to be the name as held in player registration details;
h) Account statements must be sent to the registered address of the player either on request and to the player's e-mail address on a monthly basis Statements must include sufficient information to allow the player to reconcile the statement against their own records to the session level;

Copyright © 2011 GLI Interactive BV All Rights Reserved.

i) Any adjustments to player accounts on the Gaming Platform must be subject to strict security control and audit trail;
j) It shall not be possible to transfer credits which represent a monetary value between two user accounts; and
k) Credits that are used for "Play for Fun" games and hold no monetary value may be transferred between any numbers of user accounts.

3.3 Player Game Session

3.3.1 ***General Statement***. A game session is started when a player logs in to the Gaming Platform. Game play which requires monetary payment can only occur during a game session. Where an operator provides access to multiple games from a games lobby, players may play more than one game during a game session.

3.3.2 ***Player Identification***. Player identification must meet the following rules:

a) A player must be provided with an electronic identifier such as a digital certificate or an account description and a password to start a game session; and
b) The Gaming Platform must allow players to change their passwords, and should remind them on a regular basis.

3.3.3 ***Game Session End***.

a) A game session finishes if:
    i) The player notifies the Gaming Platform that the session is finished (e.g. "logs out");
    ii) A user-inactivity timeout is reached;
    iii) The Gaming Platform host does not get a response to polls within 30 seconds to the end player device, if applicable; or
    iv) The operator terminates the session.
b) Where the operator terminates a session, a record must be written to an audit file that includes the termination reason;
c) The Gaming Platform must attempt to send a session finished message to the end player

Copyright © 2011 GLI Interactive BV All Rights Reserved.

device each time a session is terminated by the Gaming Platform.

3.4 Player Loyalty Programs

3.4.1 ***General Statement***. The requirements of this section only apply if player loyalty promotions involve the use of player loyalty to affect the taxation basis of the operator, e.g. conversion of player loyalty points into game play or redeemed as cash. If supported by the Gaming Platform, the following principles must apply:

a) The player loyalty database must be maintained on a secure part of the Gaming Platform;
b) Use of the player tracking data must not breach the operator's Privacy Policy.
c) Redemption of player loyalty points earned must be a secure transaction that automatically debits the points balance for the value of the prize redeemed; and
d) All player loyalty database transactions are to be recorded as critical data by the Gaming Platform.
e) If the Player Loyalty program is provided by an external service provider the Gaming Platform must be capable of securely communicating with that service.

3.5 Responsible Gaming

3.5.1 ***Responsible Gaming Page***. A responsible gaming page must be readily accessible from any screen where game play may occur. The responsible gaming page must contain at a minimum:

a) Information about potential risks associated with gambling, and where to get help for a gambling problem,
b) A list of the responsible gaming measures that can be invoked by the player, such as session time limits and bet limits, and an option to enable the player to invoke those measures,
c) A link to the terms and conditions the player agreed to be bound to by entering and playing on the site,
d) A link to the operator's privacy policy,
e) A link to the home website of the Regulatory Body,

Copyright © 2011 GLI Interactive BV All Rights Reserved.

f) All information in (a) and (c) should be available in languages that primarily reflect the customer base. Reasonable efforts should be made to make information in (b) available in languages that reflect the customer base.
g) An easy and obvious mechanism to advise the player of the right to make a complaint against the operator, and to enable the player to notify the Regulatory Body of the making of such a complaint. This must include a link to the Regulatory Body home page.

3.5.2 Third Party Services. All links to problem gambling services provided by third parties are to be regularly tested by the operator. Where the service is no longer available or not available for a significant period of time, the operator must provide an alternative support service.

3.5.3 Reserved.

3.5.4 Self-Exclusion. Players must be provided with an easy and obvious mechanism to self-exclude from game play, and this self-exclusion mechanism must provide the following functionality:

a) At a minimum, this self-exclusion mechanism must be accessible from the responsible gaming page.
b) The player must be provided with the option to self-exclude temporarily for a specified period of time as defined in the Terms and Conditions, or permanently.
c) In the case of temporary self-exclusion, the Gaming Platform 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, and
    ii) During the temporary self-exclusion period, the player is not prevented from withdrawing any or all of their account balance through the account management console, provided that the Gaming Platform acknowledges that the funds have cleared.
d) In the case of permanent self-exclusion, the Gaming Platform must ensure that:

Copyright © 2011 GLI Interactive BV All Rights Reserved.

i) Immediately upon receiving the self-exclusion order, no new bets or deposits are accepted from that player, until such time as the permanent self-exclusion has been revoked,
ii) The player is paid in full for their account balance, provided that the Gaming Platform acknowledges that the funds have cleared, and
iii) Players are provided with a mechanism to revoke the self-exclusion order, using a special process to be identified by the operator.

3.5.5 Involuntary Exclusion. The Gaming Platform must provide a mechanism by which the operator's staff can exclude a player from playing according to the operator's Terms and Conditions agreed to by the player upon registration. This mechanism must:

a) Include a register of reasons for the exclusion;
b) Ensure that 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 that the Gaming Platform acknowledges that the funds have cleared, and that the reason(s) for exclusion would not prohibit a withdraw; and
d) Any such exclusion may only be lifted on application by the player

3.5.6 Self-Limitation. Players must be provided with an easy and obvious mechanism to self-limit their game play, and this self-limitation mechanism must provide the following functionality:

a) At a minimum, this self-limitation mechanism must be accessible from the responsible gaming page.
b) Immediately upon receiving any self-limitation order, the gaming platform must ensure that all specified limits are correctly implemented in the Gaming Platform.
c) It is acceptable that self-limitations take effect the next time the player logs in to the gaming platform; however, the player must be clearly informed that this is the case upon setting the limit.
d) The self limitations set by a player must not override any limitations set by the operator

Copyright © 2011 GLI Interactive BV All Rights Reserved.

or the game rules.

e) Once established by a player, it must only be possible to reduce the severity of self-limitations upon seven days notice.
f) Self-limitations must not be compromised by external time events, such as leap-years and daylight savings adjustments.
g) Self-limitations must not be compromised by internal status events, such as self-exclusion orders and self-exclusion revocations
h) The self-limitation mechanism should include (but not necessarily be limited to) the following options:
    i) Bet limit per time period – an overall maximum bet limitation over a specified period of time (e.g.: daily, weekly, etc…),
    ii) Loss limit per time period – an overall maximum loss limitation over a specified period of time (e.g.: daily, weekly, etc…),
    iii) Deposit limit per time period – an overall maximum deposit limitation over a specified period of time (e.g.: daily, weekly, etc…),

3.5.7 ***Involuntary Limitation***. It is acceptable for the operator to set limits (such as those listed above) on players, and vary those limits from time to time. Any operator-imposed limits must be consistent with those described in the Terms and Conditions signed by the player. Players must be notified in advance of any operator-imposed limits unless otherwise required by regulator.

a) Immediately upon receiving any operator set imitation order, the gaming platform must ensure that all specified limits are correctly implemented in the Gaming Platform.
b) It is acceptable that operator set limitations take effect the next time the player logs in to the gaming platform; however, the player must be clearly informed that this is the case.
c) The limitations set by the operator must not reduce the severity of any limitations set by the player.
d) The operator limitation may not extend beyond seven days, except as required by jurisdictional rules and regulation, or standards where Gaming Platform is approved for use.
e) Operator-imposed limitations must not be compromised by external time events, such as

Copyright © 2011 GLI Interactive BV All Rights Reserved.

leap-years and daylight savings adjustments.

f) Operator imposed limitations must not be compromised by internal status events, such as self-exclusion orders and self-exclusion revocations.

3.5.8 Reporting Suspicious Player Activity. There must be a simple and clear method for a player to report any suspicious player activity, which must be accurately explained in the help menus and/or on the website. (e.g. the player could right click on an account name in the game window and hit an option "Report Suspicious User Activity" which brings up a new window with a form the user can fill out to give all the necessary details, including time of incident, reason the user was reported, etc…)

Copyright © 2011 GLI Interactive BV All Rights Reserved.

CHAPTER 4

4.0 Reserved

Copyright © 2011 GLI Interactive BV All Rights Reserved.

CHAPTER 5

5.0 Game Requirements

5.1 Game Design

5.1.1 ***Reserved***.

5.1.2 ***Game Rules***. The following requirements apply to game rules displayed to the player:

a) The rules of the game must be available to the player directly on the game interface or accessible from the game interface via a hyperlink;
b) All game rules and paytable information should be accessible by a player prior to committing to a bet;
c) The published game information must be sufficient to explain all of the applicable rules and how to participate in the game;
d) The rules of the game shall not be unfair or misleading;
e) The game must operate and interact with the player in accordance with the rules displayed to the player;
f) Game rules must not be changed during a session unless effective notification is given to the player. Games rules cannot be changed between a player committing a wager and the decision resulting in the payment of winnings for the wager and;
g) A rule change constitutes a different game, although variations to the maximum number of credits bet per game (and/or lines per game) are permitted. This requirement does not preclude implementations of games with multiple parts or features provided that the rules are clear to the player.

5.1.3 ***Reserved***

5.1.4 ***Maximum Prize***. The maximum prize paid out by gaming software shall be as specified in the game rules and shall be displayed within the help screens for that particular game.

Copyright © 2011 GLI Interactive BV All Rights Reserved.

5.1.5 ***Maximum Stake***. The maximum stake shall be as specified in the game rules and shall be displayed within the help screens for that particular game.

5.2 Game Artwork

5.2.1 ***Reserved***

5.2.2 ***Game Information***. The following game information shall be visible or easily accessible to the player at all times from either a help menu or website:

a) The name of the game being played;
b) Instructions on how to play, including a paytable for all prizes and special features;
c) Restrictions on play or betting such as any play duration limits, maximum win values, etc;
d) The player's current credit balance;
e) The current bet amount. This is only during the base game or if the player can add to the bet during the game;
f) The denomination of the bet and, where applicable, any tokenization implemented in the game;
g) All possible winning outcomes, or be available as a menu item or on the help menu;
h) Win amounts for each possible winning outcome, or be available as a menu or help screen item;
i) The amount won for the last completed game (until the next game starts or betting options are modified);
j) The player options selected (e.g., bet amount, lines played) for the last completed game (until the next game starts or a new selection is made);
k) Initial player selection options are to be described (e.g. selection of a runner in a horse race should identify name, number and expected payout). Player selection options once the game has commenced should be clearly shown on the screen;
l) The winning amount for each separate wager and total winning amount are to be displayed on the screen;
m) The minimum theoretical %RTP and explanation on how calculated (e.g. Total prizes for game cycle divided by total number of different outcomes in game cycle).

Copyright © 2011 GLI Interactive BV All Rights Reserved.

***NOTE**: This requirement does not apply to games where there is sufficient information available to the player to enable the player to readily and easily determine the house edge or percentage return to player.*

n) Whether there are contributions to jackpots ("progressives") and the way in which the jackpot operates, for example, whether the jackpot is won by achieving a particular outcome;

o) Any rules pertaining to the metamorphosis of games, for example, the number and type of tokens that need to be collected in order to qualify for a feature or bonus round and the rules pertaining to that bonus round where they may otherwise differ from the base game; and

p) The following information must be readily available to the player (i.e. displayed directly on the game "page" or accessible via a hotlink on the page):

   i) Information on responsible gambling, including instructions on how to limit bets per game and/or session and invoke self-exclusion arrangements; and

   ii) Information on contact points for problem gambling services.

5.3 Peer to Peer (P2P) Games

5.3.1 General Statement. P2P game rooms are those environments which offer players the opportunity to gamble with and against each other. In these environments, the operator usually does not engage in the gambling event as a party (e.g. house banked gaming), but usually provides the gambling service or environment for use by its players, and takes a rake, fee, or percentage for the service.

5.3.2 P2P Game Rules. The following requirements apply to P2P games:

a) The operator must clearly describe the operator's Terms and Conditions used for registering an account.

b) The customer should not be allowed to play against himself where the customer has an ability to influence the outcome of the game.

c) A player may only occupy one seat at any individual table.

d) The operator's collusion policy, including possible sanctions must be clearly described to

Copyright © 2011 GLI Interactive BV All Rights Reserved.

the player.

e) The operator must provide warnings about how bots can affect play, so that customers can make an informed decision whether to participate.
f) In order to avoid collusion by players sitting at both ends of the table or in some other supportive seating arrangement, random table allocation is vital in both sit-n-go and multi-table tournaments. However, random table allocation is not required on ring tables, as players prefer to choose their playing partners;
g) The rules must clearly describe the procedure in case of player disconnection from the network server during a game (e.g. internet connection outage, PC crash, etc.)
h) The house percentage and other gambling service fees ("rake"), must be clearly explained and displayed to the player.

5.3.3 Computerized Players. The following requirements apply to use of computerized players:

a) The software may employ the use of Artificial Intelligence (AI) in order to fill up multi-player tables.
b) The use of AI software must be clearly explained in the help menus.
c) The use of AI software may only be used upon player request and may not be used by the software to automatically fill empty table seats.
d) All AI players must be clearly marked at the tables so that players are aware of which players are not human.
e) Any artificial intelligence used to fill in game tables must not have a tactical advantage against the average human player. (i.e. They may not communicate with the server to see what other cards the players are holding in order to determine the next action taken).
f) Steps to report suspected player-bot usage from a player must be clearly explained in the help menus.

5.4 Game Play

5.4.1 General Statement. The following rules pertain to the game play:

a) Hotlinks used to supply game information such as game rules and paytables, must be

Copyright © 2011 GLI Interactive BV All Rights Reserved.

checked daily.

b) An invitation to play a particular game must only be extended if the Gaming Platform determines that the encrypted communications channel to the end player device is adequate for that game, and the end player device has sufficient capabilities to play the game (e.g. check the version number of the web browser and/or the version number of the game client).
    i) If the software is designed so that players may invite each other to play a particular game, or sit at a particular table, the software must prohibit any one player from sending an invitation to more players than the game allows, or seats that are open at the current table.
    ii) Invitations to play must require a person to either accept or discard the invitation. If no action has been taken by the recipient after five minutes, decline must be automatically selected by the software.
    iii) Once a player declines an invitation, the player that sent the invite shall be notified and subsequently be permitted to invite another player.
    iv) The software shall prohibit the player from choosing the wording of an invitation. The player may choose from a variety of options, which will generate a standardized invitation (i.e. “Player1 has sent you an invitation to play Texas Hold’em at table number 1111, which has a minimum bet of 20 credits and a no-limit maximum bet.”, or “Player1 has sent you an invitation to play Texas Hold’em at a new table. You will be able to discuss the table options in the pre-game lobby”, etc…).
c) For multi-player games where the result is affected by the time to respond to a game event, the Gaming Platform must only offer the game after informing the player of any handicap associated with the communication channel. Games that are inherently unfair will not be approved.
    i) All multiplayer games must be equipped with a latency meter which allows the player to readily determine the strength of the end user’s connection to the server
    ii) This can be displayed via any appropriate method, such as displaying the ping time in milliseconds, the display of “high”, “medium”, and “low” in regards to

Copyright © 2011 GLI Interactive BV All Rights Reserved.

latency, the use of red, yellow, and green for speed of connection, etc...

d) If a cookie is required to be accepted for game play, an invitation to play may only be extended if the Gaming Platform determines that the end play device can accept them.
    i) All cookies used shall contain no malicious code.
e) The client software must not operate if sufficient resources are not available to it. The player must be informed of the minimum Gaming Platform specifications required to correctly run the client software. Visual instructions must accompany any sound used to provide instructions on how to play games.
f) If the Gaming Platform extends an invitation to play a particular game, it must accept all legitimate wagers for that game.
g) There must exist a Game Selection Menu where the full amount of the player's session balance is displayed in currency or credits. If a player's session balance is different from the total funds held by the provider on the player's behalf it must be unambiguous to the player that they are different. On a player's session balance becoming zero or less than an amount necessary to place a bet or on the player exiting the game being played the player's total funds are to be displayed.
h) The methodology employed by a player to select and play a particular game must be unambiguous.
i) The Gaming Platform must clearly inform the player of all games available at that time.
j) The player must at all times be made aware of which game has been selected for play or is being played.
k) The player must not be forced to play a game just by selecting that game.
l) It must not be possible to start a new game before all relevant meters have been updated on the Gaming Platform and all other relevant connections and session balance, or if applicable, player's total funds balance, has been updated.
m) A gaming device shall only initiate game play:
    i) After credits have been registered, and
    ii) After the player has nominated the number of credits to bet on that game, and
    iii) After the player presses a "play" button (or similar input).
n) If an auto play mode is incorporated, it shall be possible to turn this mode off at any time

Copyright © 2011 GLI Interactive BV All Rights Reserved.

during game play.

5.4.2 ***Incomplete Games***. The following requirements apply to incomplete games:

a) A game is incomplete when the game outcome remains unresolved or the outcome cannot be properly seen by the player. Incomplete games may result from:
   i) Loss of communications between the Gaming Platform and the end player device;
   ii) A Gaming Platform restart;
   iii) An end player device restart;
   iv) A game disable by the Gaming Platform during play; or
   v) Abnormal termination of the gambling application on the end player device.

b) The Gaming Platform must provide a mechanism for a player to complete an incomplete game.

c) Upon reconnection by the player, the Gaming Platform must present the player the incomplete game for completion:
   i) Where no player input is required to complete the game, the game must display the final outcome as determined by the RNG and game rules, and the player`s account must be updated accordingly;
   ii) For single-player games, where player input is required to complete the game, the game must return the player to the game state immediately prior to the interruption and allow the player to complete the game; and
   iii) For multi-player games, the game must display the final outcome as determined according to the operator`s rules for multi-player games, and the player`s account must be updated accordingly.

d) Bets associated with a partially complete game that can be continued must be held by the Gaming Platform until the game completes. Player accounts must reflect any funds held in incomplete games.

e) The operator`s Terms and Conditions must specify that bets placed but remaining undecided in incomplete games will become void after a specified time, and will be forfeited.

Copyright © 2011 GLI Interactive BV All Rights Reserved.

CHAPTER 6

6.0 Jackpot (Progressive) Requirements

6.1 Introduction

6.1.1 ***General Statement***. A Jackpot (Progressive) is an increasing prize, based on a function of credits that are bet. This includes prizes that are awarded based on criteria other than obtaining winning outcomes in the game, such as 'Mystery Jackpots.' However, this does not include prizes that result from bonus features which are part of the game theme, which offer prizes that increase as the game is played and, as well, is not configurable.

6.2 Jackpot Design and Operation

6.2.1 ***Jackpot Fairness***. In order to have a jackpot that is fair to players the following principles must apply:

a) All players that play jackpot games must be made aware of actions which would make them eligible to win the jackpot.
b) Where jackpot contributions are part of the %RTP calculation, the contributions must not be assimilated into revenue. If a cap is established on any jackpot all additional contributions once that cap is reached are to be credited to a Diversion Pool. The minimum return to player must be achieved regardless of the number of betting units calculated.
c) The rules of the game must incorporate how the jackpot is funded and determined.
d) If a minimum bet amount exists in order for a player to win a linked jackpot, then the base game (excluding the jackpot) must meet the minimum player return.
e) The current jackpot amount should be displayed on all end player devices participating in the Jackpot. This display should be updated on all participating end player devices at least every 30 seconds.

Copyright © 2011 GLI Interactive BV All Rights Reserved.

***NOTE**: It is accepted that, depending upon the medium, communication delays are variable and beyond the knowledge or control of the operator. Server-to-client delays will vary from player to player and from message to message.*

6.2.2 Jackpot Financial Liability Documentation. The rules of the game shall provide for the following:

a) Procedures for the disposition of any outstanding pool amounts in the event of a planned jackpot termination; and
b) Procedures for the administration of the jackpot pool including positive or negative jackpot pool balance in the event of an unplanned jackpot termination.

6.2.3 Jackpot Controller. The jackpot controller is deemed part of the Gaming Platform even if it is one or more physically separate devices.

a) Where a "Master Controller" employs "Slave Controllers" to control a Jackpot the following requirements apply:
    i) All Slave Controllers must be time synchronized with the Master Controller,
    ii) The Master Controller must be time synchronized with the Gaming Platform, and
    iii) Jackpot win events must be time-stamped and the Jackpot Controller must ensure that hits registered within a minimum time increment are considered as simultaneous wins. Prize payout for simultaneous wins is to be made in accordance with the Rules of the game.
b) The minimum time window (Jackpot Reset Period) is not less than the longest time taken to:
    i) Register that a jackpot has been won,
    ii) Announce the win on the displays of all participating end player devices with an active session, and
    iii) Reset the progressive meters.
c) If supporting a jackpot that is determined by increments of individual player's wagers, the processing of receipt of increments from all end player devices, whether attached to Master or Slave controllers, must be fair.

Copyright © 2011 GLI Interactive BV All Rights Reserved.

6.2.4 Voided Jackpots. Voided jackpots must be returned to the jackpot pool as soon as practical. Procedures regarding the decision to void a Jackpot must conform to the applicable regulatory requirements.

6.2.5 Jackpot Win Notification. The following requirements must be met when there is a jackpot win:

a) A winning player must be notified of a jackpot win by the end of the game in play;
b) The notification of the jackpot being won must be provided to all end player devices participating in the jackpot at the time of the jackpot win;
c) The jackpot amount must be displayed on all end player devices participating in the jackpot at the time of the jackpot win; and
d) The jackpot win notification should also display the value to which the jackpot is being reset.

6.2.6 Multiple (Simultaneous) Jackpot Winners. The operator must address the possibility of a 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.

6.2.7 Jackpot Parameter Changes. The following requirements apply to configuring jackpots:

a) Once a Jackpot has commenced, parameter changes must not take effect immediately - rather they should be saved to apply after the current Jackpot is won. These are 'pending' parameters.
b) A Mystery Jackpot which uses a hidden jackpot amount to determine the jackpot win must not change the hidden jackpot amount when the parameters are changed if the jackpot is active (i.e. had any jackpot contributions added to it).
c) The Gaming Platform must provide a means of displaying current and pending jackpot parameters.
d) The Gaming Platform must record the values of all jackpot meters, as well as all of the "Current" and "Pending" jackpot parameters.

6.2.8 Partial Jackpot Redirection. Diversion Pool schemes, where a portion of the jackpot contributions are redirected to another pool so that when the jackpot is won, the Diversion Pool is added to the seed of the next jackpot, are acceptable.

Copyright © 2011 GLI Interactive BV All Rights Reserved.

6.2.9 Jackpot Shutdown. There are instances where a jackpot should be shut down. The following requirements shall apply in the event of a jackpot shutdown:

a) Clear indication must be given to players that the jackpot is not operating (e.g. by displaying "Jackpot Closed" on end player devices).
b) It must not be possible for the jackpot to be won while in the shutdown state.
c) If the jackpot operates in conjunction with another game (e.g. base game) and the player return requirement is only met when jackpot contributions are included the other game may only be offered when the jackpot is available.
d) Activation of the jackpot from the shutdown state must return the jackpot with the identical parameters including jackpot value, and hidden win amount for mystery jackpots, as before the shutdown.

6.2.10 Jackpot Recovery. To enable recovery of the current value of the progressive jackpot amount(s) in the case of a Gaming Platform or jackpot controller failure, either:

a) The current value of the progressive amount must be stored in at least two physically separate devices, or
b) The current value of the progressive amount must be able to be accurately calculated from other available metering information, which is not stored in the same Gaming Platform as the progressive amount.

In either case, all eligible jackpot winners must be paid as soon as the value is recovered.

6.2.11 Jackpot Contributions. The rules of the game must clearly specify how the contributions to the jackpot pool are made (based on turnover, net balance of each operator contributing to a multi-operator pool, etc).

6.2.12 Multi-Operator Jackpots. Multi-operator Jackpots will be considered on a case-by-case basis.

6.2.13 Jackpot Accounting. If the calculation of gross revenue for taxation purposes allows for jackpot contributions to be totally deductible (as opposed to deducting jackpot prizes when paid), the Gaming Platform must provide adequate reconciliation to ensure that all jackpot increments deducted:

a) Have been paid to players as prizes; or

Copyright © 2011 GLI Interactive BV All Rights Reserved.

b) Are displayed as part of prizes; or

c) Are held in accountable reserves (which can be demonstrated) to be paid to players in the future, (i.e. as part of future prizes).

Copyright © 2011 GLI Interactive BV All Rights Reserved.

CHAPTER 7

7.0 Information Systems Security (ISS) Requirements

7.1 General Statement

To ensure players are not exposed to unnecessary security risks by choosing to participate in interactive gaming these security requirements will apply to the following critical components of the Gaming Platform:

a) Gaming Platform components which record, store, process, share, transmit or retrieve sensitive customer information, e.g. credit/debit card details, authentication information, customer account balances;
b) Gaming Platform components which generate, transmit, or process random numbers used to determine the outcome of games or virtual events;
c) Gaming Platform components which store results or the current state of a customer's gamble;
d) Points of entry to and exit from the above systems (other systems which are able to communicate directly with core critical systems); and
e) Communication networks which transmit sensitive customer information.

7.2 Information Security Policy

7.2.1 General Statement. An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties. The following requirements shall apply to the information security policy:

a) The information security policy shall be reviewed at planned intervals and/or as significant changes occur to ensure its continuing suitability, adequacy and effectiveness.
b) The operator's approach to managing security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned interval, or when significant changes to the security

Copyright © 2011 GLI Interactive BV All Rights Reserved.

implementation occur. Examples of "significant changes" could include an upgrade to an operating system, allowing access to the Gaming Platform by external sources, addition of new Gaming Platform components and network configuration changes such as the addition of new subnets.

7.3 Physical and Environmental Controls

7.3.1 Secure Areas.

a) Gaming platforms and the associated communications systems must be located in facilities which provide physical protection against damage from fire, flood, hurricane, earthquake and other forms of natural or man-made disaster.
b) Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) must be used to protect areas which contain information processing systems.
c) Secure areas must be protected by appropriate entry controls to ensure that access is restricted to only authorized personnel.
d) All access must be recorded in a secure log.
e) Secure areas must include an intrusion detection system, and attempts at unauthorized access must be logged.

7.3.2 Equipment Security.

a) Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
b) Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
c) Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

7.3.3 Incident Management.

a) Policies, plans and procedures should be in place to address the management of any security incidents.

Copyright © 2011 GLI Interactive BV All Rights Reserved.

7.4 Administrative Controls

7.4.1 Human Resource Security.

a) All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

b) The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

7.4.2 Third Party Services.

a) Agreements with third parties involving accessing, processing, communicating or managing the operator's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.

b) The services, reports and records provided by the third party shall be monitored and reviewed, and audits shall be carried out at least once a year.

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

7.4.3 Backup Policy.

a) Backup copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.

7.4.4 Media Handling.

a) Procedures must be in place for the management of removable media.

b) All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

c) Media shall be disposed of securely and safely when no longer required, using formal procedures.

d) Procedures for the handling and storage of information shall be established to protect this

Copyright © 2011 GLI Interactive BV All Rights Reserved.

information from unauthorized disclosure or misuse.

e) Gaming Platform documentation shall be protected against unauthorized access.

7.4.5 Patch and Update Management.

a) A written policy for the implementation of all software patches and updates must be in place.

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

7.4.6 Change Control Procedures.

a) Program change control procedures must be adequate to ensure that only properly approved and tested versions of programs are implemented on the production Gaming Platform. Production change controls must include:

i. An appropriate software version control or mechanism for all software components;

ii. Details of the reason for the change;

iii. Details of the person making the change; and

iv. Complete backups of previous versions of software.

7.4.7 Authentication.

a) All people (e.g. players, computer operators, maintenance service providers, jurisdiction officers and representatives) and computer systems (e.g. jackpot controllers, financial gateway systems, certification authority systems) that connect to the Gaming Platform must be authenticated except as provided in item (b) below.

b) Players who connect to the Gaming Platform for purposes other than gambling do not need to be authenticated unless sensitive account information (i.e. monetary transactions, personal information etc…) is being accessed.

c) The Gaming Platform must authenticate itself to all people and computer systems that establish a connection.

Copyright © 2011 GLI Interactive BV All Rights Reserved.

d) Authentication of people, computer systems controlled by the operator and third party Gaming Platforms must be based on a certification authentication method recognized by the Jurisdiction as being currently secure.

e) Where a player has forgotten their password/PIN, the Gaming Platform must provide a secure process for the re-authentication of the player and the retrieval and/or resetting of the password/PIN.

7.4.8 Software Development, Testing, Maintenance and Service.

a) Cross-platform software must have identical code for each version, with the exception of operating system dependent functionality.

7.4.9 Code Security.

a) Closed Source Software. Where appropriate code should be protected as much as possible from the player.

b) Open Source Software. If the software is being submitted as an open source project:

   i. The developers of the software must obtain a valid open source programming license in order to be classified as an open source submission.

   ii. A valid procedure must be implemented, which does not violate the open source software license obtained, in order to prevent individuals from publicly publishing their own code modifications that alter the security and integrity of the software and Gaming Platform.

   iii. The Gaming Platform must be able to reasonably detect any end user made code modifications, and prevent the software from running if any modifications can alter the integrity of the game and/or Gaming Platform.

c) Customizable Aspects Through Code Changes: If the client software allows for user customization (e.g. customizable decks of cards), then the following requirements must be met:

   i. The game client may allow for user customization (i.e. interface skinning, customized card decks, etc…). However, should the method of customization be implemented through code modifications, the code must only consist of markup languages.

   ii. No programming languages may be used for this purpose, which are able to

Copyright © 2011 GLI Interactive BV All Rights Reserved.

perform Gaming Platform level commands.

d) Any publicly installable theme packages must be hosted and monitored on the official website for the game, and all themes uploaded must be verified to ensure they contain no potential exploits or malware.

7.5 Technical Controls

*7.5.1 **Reserved***.

*7.5.2 **Domain Name Service (DNS) Requirements***.

a) An operator of a Gaming Platform must register a recognizable name (e.g. company.com) in the Internet Domain Name Server (DNS). The Gaming Platform itself must be registered in the DNS;

b) The primary server used to resolve DNS queries (i.e. forward and reverse lookups) used in association with the Gaming Platform must be controlled by the operator and physically located in the secure data center;

c) Logical and physical access to the primary DNS server must be restricted to authorized personnel;

d) There must be at least one secondary server that is able to resolve DNS queries (i.e. forward and reverse lookups). The secondary servers must be located at a separate premises to the primary server; and

e) Zone transfers between the primary server and the secondary servers must occur at least every 24 hours.

*7.5.3 **Self-Monitoring***.

a) The Gaming Platform must implement the self-monitoring of critical components (e.g. central hosts, network devices, firewalls, links to third parties, etc.).

b) A critical component which fails self-monitoring tests must be taken out of service immediately. The component must not be returned to service until there is reasonable evidence that the fault has been rectified.

*7.5.4 **Protection from Attacks***.

a) All reasonable precautions must be taken to protect the Gaming Platform against attacks

Copyright © 2011 GLI Interactive BV All Rights Reserved.

based upon the replay of authentic or non-authentic messages (for example, Distributed Denial of Service Attack).

b) The software must be able to reasonably detect and/or prevent a man-in-the-middle style attack without invading the end user's privacy.

c) If a man-in-the-middle attack has been suspected, all communications between the suspected client and server must be terminated with a message displayed to the end user as to why communications were terminated.

d) Upon termination of client-server communications, the appropriate steps to determine if the end user was performing a man-in-the-middle attack. If it was determined that a man-in-the-middle attack was attempted, the appropriate actions in regards to cheating must be taken.

e) All reasonable precautions must be taken to ensure that no data kept on the Gaming Platform or transferred by it can be infected with a virus program, Trojan Horse, worm, or other malware.

f) Penetration testing of the Gaming Platform must be performed at least once every six months.

7.5.5 Network Security Management.

a) Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

b) Internal vulnerability scans on network components should be performed at least once every six months.

c) Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

7.5.6 Network Access Controls.

a) An access control policy shall be established, documented, and reviewed based on business and security requirements for access.

b) A formal user registration and de-registration procedure must be in place for granting and revoking access to all information systems and services.

Copyright © 2011 GLI Interactive BV All Rights Reserved.

c) The allocation of user privileges shall be restricted and controlled based on business requirements.
d) Management shall review users' access rights at regular intervals using a formal process.
e) Users shall only be provided with access to the services that they have been specifically authorized to use.
f) Passwords must be controlled through a formal management process.
g) The selection of passwords must follow good security practices.
h) Unattended equipment shall have appropriate protection and automatically log the user out after a pre-determined interval.
i) Appropriate authentication methods shall be used to control access by remote users.
j) Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.
k) Physical and logical access to diagnostic and configuration ports shall be controlled.
l) Groups of information services, users, and information systems shall be segregated on networks.
m) For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications.
n) Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

7.5.7 Operating System Access Controls.

a) Access to operating systems shall be controlled by a secure log-on procedure.
b) All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.
c) Systems for managing passwords shall be interactive and shall ensure quality passwords.
d) The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
e) Inactive sessions shall shut down after a maximum of 30 minutes of inactivity.
f) Restrictions on connection times shall be used to provide additional security for high-risk

Copyright © 2011 GLI Interactive BV All Rights Reserved.

applications.

g) Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.

h) Sensitive systems shall have a dedicated (isolated) computing environment.

i) A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.

j) A policy, operational plans and procedures shall be developed and implemented for telecommuting activities.

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

a) Where sensitive data is being passed over communication lines, such data must be encrypted. Examples of data that may require encryption are PINs or passwords, account numbers (including card numbers) and details, encryption keys, player identity details, funds transfers to and from customer accounts, changes to account details (e.g.: change of address, change of credit card, change of name, etc.), and game play (i.e.: games played, amounts bet, amounts won, jackpots won etc.).

b) Data that is not required to be hidden but must be authenticated must use some form of message authentication technique;

c) Sensitive data must be encrypted on an end-to-end basis (i.e. the data must never appear on a LAN or WAN in an un-encrypted form). This includes sensitive data transmitted between computer Gaming Platforms within an operator's premises;

d) Sensitive data transmitted between Gaming Platforms on a switched network within a single secure data center need not be encrypted;

e) Sensitive data transmitted between Gaming Platforms that are located within separate secure data centers need not be encrypted if the communications path is physically secure and cannot be access by unauthorized people;

f) All communications between operator terminals and the Gaming Platform must be strongly authenticated and strongly encrypted during transmission outside their respective secure data centers; and

g) Authentication must be available via a Secure Socket Link (SSL) and a security certificate from an approved organization.

Copyright © 2011 GLI Interactive BV All Rights Reserved.

h) Encryption algorithms are to be demonstrably secure against cryptanalytic attacks;

i) Operators must have approved procedures for following up reports of weaknesses in encryption algorithms used in any part of the Gaming Platform (including, but not limited to, RNGs, firewalls, authentication systems and operating Gaming Platform). Changes to encryption algorithms to correct weaknesses must be implemented as soon as practical. If no such changes are available, the algorithm must be replaced.

7.5.9 Cryptographic Key Management.

a) The minimum width (size) for encryption keys is 112 bits for symmetric algorithms and 1024 bits for public keys.

b) There must be a secure method implemented for changing the current encryption keyset. It is not acceptable to only use the current key set to "encrypt" the next set. An example of an acceptable method of exchanging keys is the use of public key encryption techniques to transfer new key sets.

c) There must be a secure method in place for the storage of any encryption keys. Encryption keys must not be stored without being encrypted themselves through a different encryption method and/or by using a different encryption key.

7.5.10 Malicious and Mobile Code.

a) Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.

b) Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.

7.5.11 Monitoring.

a) Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.

b) Any modification, attempted modification, read access or other change or access to any Gaming Platform record, audit or log must be noticeable by an approved Gaming Platform via version control or file time stamping. It must be possible to see who has

Copyright © 2011 GLI Interactive BV All Rights Reserved.

viewed or altered a log and when.

c) Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed quarterly or as required by the jurisdiction.
d) Logging facilities and log information shall be protected against tampering and unauthorized access.
e) System Administrator and System Operator activities shall be logged.
f) Faults shall be logged, analyzed, and appropriate action taken.
g) The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.

7.5.12 Communications Security Management. This section refers to communications between the host Gaming Platform and an end player device, but it also applies to communications between other components or equipment of the Gaming Platform.

a) Message authentication must be used with critical message types, such as jackpot wins and password/PIN transmissions, in order to verify the correct receipt of the message by the end player device, host or related equipment. A protocol that doesn't correct errors or re-send erroneous packets (e.g. UDP) may be used as long as no critical game data or information is sent in this manner. For example, if UDP is being used to stream video or sound then it would not be acceptable to have the game instructions or paytable in this format only.
b) The game server must be able to validate all of the information received from the client to ensure no additional data (such as a worm) has been sent.
c) If it has been detected that additional data (such as a worm) has attached itself to the received data, the game server must not allow the extraneous byte code to pass through to the Gaming Platform.
d) All protocols must use communication techniques which have proper error detection and/or recovery mechanisms and meet the following rules:
    i. The high level protocol must employ techniques (e.g. end to end acknowledgment) such that it will not lose messages – even when one end or the other restarts;

Copyright © 2011 GLI Interactive BV All Rights Reserved.

ii. These techniques must not cause either the Gaming Platform or any end player device to completely halt all processes while waiting for this acknowledgement.

e) The higher level protocol must employ techniques (e.g. transmission numbers) such that repeated messages are identified and discarded – even when one end or the other restarts;

f) These requirements do not apply to unsecured messages such as broadcast messages;

g) All functions of the protocol must be clearly specified in its documentation;

h) The following rules apply to the timestamps in a high level protocol:

i. It must include a provision for the transmitting system (i.e. Gaming Platform or end player device) to insert a local timestamp in every message it sends. This timestamp will assist in claims of equipment malfunction involving run away hardware or software; and

ii. It must include a provision for the transmitting system (i.e. Gaming Platform or end player device) to insert a local timestamp taken at the time the last valid high level message was received.

i) The following requirements apply to High Level Interface with Lower Level Protocols:

a) There must be no restrictions placed on characters that may be included in messages passed to or from the higher levels to the lower levels;

b) The interfaces between the high layer protocols and the low layer protocols must cater for messages of variable length including those longer than the standard buffer size of the lowest level;

c) A method of flow control to prevent loss of vital messages must be implemented;

d) The Gaming Platform shall detect the maximum transfer speed between it and the player's environment and notify the player if the speed detected falls below the minimum requirement set by the Regulator responsible for the player's Jurisdiction; and

e) This information shall be displayed to the player via a latency meter which fits the requirements listed within this document.

7.5.13 Firewalls. The following requirements apply to firewalls:

a) All connections to Gaming Platform hosts in the secure data center must pass through at

Copyright © 2011 GLI Interactive BV All Rights Reserved.

least one approved application-level firewall. This includes connections to and from any non-Gaming Platform hosts (e.g. MIS computer Gaming Platforms) used by the operator. The term "connections" is used in its broadest sense, and includes UDP and TCP data transfers;

b) The choice of firewall will be affected by the low-level protocol used by the application. (e.g. some firewalls are not able to make intelligent decisions about UDP streams.) Reducing the effectiveness of the application level firewall to a packet filter will not be permitted simply due to a poor choice of firewall / low level protocol combination;

c) A device in the same broadcast domain as the Gaming Platform hosts must not have a facility that allows an alternate network path to be established that bypasses the firewall. Examples of prohibited facilities are:

- An operator PC equipped with a phone modem; and
- An operator PC with a connection to the Gaming Platform VLAN and a connection to the corporate VLAN.

d) The firewall must be a separate hardware device with the following characteristics:

i. Only firewall-related applications may reside on the firewall; and

ii. Only a limited number accounts may be present on the firewall (e.g. Gaming Platform administrators only).

e) All data packets addressed to the firewall must be rejected if they arrive on interfaces to networks which are outside the baseline envelope. This is to restrict access to the firewall to authorized workstations inside the baseline envelope;

f) The firewall must reject all connections except those that have been specifically approved by the jurisdiction;

g) The firewall must maintain an audit log of all changes to parameters that affect what connections are permitted through the firewall;

h) The firewall must maintain an audit log of all successful and unsuccessful connection attempts through itself;

i) The firewall must disable all communications if the audit log becomes full;

j) The firewall must reject all messages received on an interface if the message purports to be on a device attached to another interface;

Copyright © 2011 GLI Interactive BV All Rights Reserved.

k) Operators must have approved procedures for following reports of security incidents and for ensuring that firewalls are kept up to date with respect to advisory recommendations released after such incidents; and

l) Networks on the secure side of the firewall should use RFC1918 private network numbers. These numbers must be translated into public network numbers for transmission over the Internet.

7.5.14 Web Application Security. The following requirements apply to the security of the application used in the end player device:

a) The Gaming Platform must be able to detect the version of the web browser or client software, being used by the player at the time the player logs on.

b) If the version of the web browser or client software being used by the player does not have the capability to run the application (e.g. the game requires Flash Player 10 but the browser only has Flash Player 8), the Gaming Platform must not allow the application to be executed until the client software has been updated, and must provide a link to download any required upgrades.

Copyright © 2011 GLI Interactive BV All Rights Reserved.

Glossary

Term or Abbreviation Description

Interactive Gaming System (IGS) - The hardware, software, firmware, communications technology and other equipment which allows a player to remotely bet or wager through the Internet or a similarly distributed networking environment, and the corresponding equipment related to game outcome determination, the display of the game and game outcomes, and other similar information necessary to facilitate play of the game. The term does not include computer equipment or communications technology used by a player to access the interactive gaming system.

Gaming Platform - The interactive gaming system hardware and software which drives the features common to all games offered, and which forms the primary interface to the gaming system for both the player and the operator. The gaming platform provides the player with the means to register an account, log in to / out of their account, modify their account information, deposit and withdraw funds to / from their account, request account activity statements / reports, and close their account. In addition, any web pages displayed to the player that relate to gaming offered on the IGS, but are not an actual game screen, are considered to be part of the gaming platform. The gaming platform provides the operator with the means to review player accounts, enable / disable games, generate various gaming / financial transaction and account reports, input game outcomes for sports betting events, enable / disable player accounts, and set any configurable parameters.

Background Cycling / Activity - If the software-based RNG is cycling in the background, it means that there is a constant string of random numbers being generated by the RNG, even if they are not actually required by the game at that time. Without background cycling / activity, one could predict the result of the next iteration of the function used to produce the random numbers if the current values and the algorithm were known.

Percentage Return to Player (%RTP) - The expected percentage of wagers that a specific game will return to the player in the long run. The %RTP can be calculated via either a theoretical or simulated approach. The method used for calculation depends on the game type.

Multi-stage Game - A game having one or more intermediate steps that require player input in order to proceed. Poker and Blackjack are two examples of multi-stage games.

Mapping - The process by which a scaled number is given a symbol or value that is usable and applicable to the current game (e.g.: the scaled number 51 might be mapped to an ACE OF SPADES).

Copyright © 2011 GLI Interactive BV All Rights Reserved.

Scaling - Raw output from an RNG will normally have a range far in excess of that required for its intended use (e.g.: 32-bit RNG's have over two billion possible outcomes, but (for example) we have only to determine which of 52 cards to draw). Scaling is required to divide the raw output into smaller, and usable numbers. These 'scaled' numbers can then be mapped to particular card numbers, record numbers, symbols, etc… Consequently, raw output from an RNG will sometimes have a range far smaller than that required for its intended use (e.g.: 0 < raw output < 1). In these cases, scaling is required to expand the RAW output into larger usable numbers.

Metamorphic Game - A metamorphic game is where the rules of the game provide for the game to have 'memory' of prescribed previous events, such that these events build up over time, eventually resulting in some change in the game. For example, the game could be designed to allow the player to gather special coins or token throughout regular game play. Once enough coins / tokens are accumulated, the game enters into a special feature. Upon exiting this feature, the coins / tokens are reset to zero, allowing the player start accumulating them over again.

Random Number Generator (RNG)- The IGS hardware and / or software which determines random outcomes for use by all of the games hosted / offered on the gaming platform.

Baseline - An administrative method a taking a snapshot of an evolving system (and in some cases defining what portions of the system can be changed without approval).

Broadcast domain - The set of computer systems that are able to communicate with one another using network level broadcast packets. An example of a broadcast domain is an IP subnet.

Contributions - The financial method by which jackpot pools are funded.

Critical Component - Any sub-system whose failure or compromise can lead to loss of player entitlements, government revenue or unauthorized access to data used for generating reports for the jurisdiction.

Digital Certificate - A set of data which can be used to verify the identity of an entity by reference to a trusted third party (the Certification Authority). Digital certificates are often used to authenticate messages for non-repudiation purposes. One of the attributes of a digital certificate is that it cannot be modified without compromising its internal consistency. X.509 certificates are an example of a digital certificate.

Domain Name System - The globally distributed Internet database which (amongst other things) maps machine names to IP numbers and vice-versa.

Effective bandwidth - The amount of data that actually can be transferred across a network per unit of time. The effective bandwidth through the Internet is usually considerably lower than the bandwidth of any of the constituent links.

End Player Device - The device that converts communications from the Gaming Platform into a human

Copyright © 2011 GLI Interactive BV All Rights Reserved.

interpretable form, and converts human decisions into communication format understood by the Gaming Platform. Examples of End Player Devices include personal computers and telephones.

Hotlink - A word or graphic on a web page which, if clicked, causes a different information page to be displayed.

ICMP - Internet Control Message Protocol. Part of the TCP/IP communications protocol which is used to measure and control devices at the IP level. ICMP echo request and ICMP echo reply are commonly and collectively known as "ping" or "trace route".

Increment Rate - The portion of the jackpot contributions that are incrementing the jackpot (as compared to funding the startup value).

Link utilization - The percentage time that a communications link is engaged in transmitting data.

Mystery Linked Jackpot - A type of jackpot where a randomly selected trigger point is chosen between a jackpot start-up amount, and a maximum win amount. A win is triggered when contributions to the jackpot increment the startup value to the trigger amount.

Pool - An accumulated reservoir of jackpot monitory contributions.

Progressive Linked Jackpot - A type of jackpot where the Gaming Platform triggers the jackpot prize (the prize being a pool of contributions from a group of machines participating in the jackpot).

Protocol - Used to refer to the hardware interface, line discipline and message formats of the communications.

Sensitive data - Data which, if obtained by a third party, may be used to affect game outcome/s or player/s accounts.

Signature Check - A security mechanism a CMCS uses to verify SW in peripheral devices or end player devices.

Soft gambling product - A gambling product that meets the published set of criteria for "soft" gambling products or receives special approval under the National Regulatory Model.

Startup value - The initial jackpot value (does not include values from overflow meters).

Time Based Jackpots - A type of jackpot where a randomly selected trigger time is chosen between a jackpot run start time and the jackpot run end time.

Timestamp - A record of the current value of the Gaming Platform date and time which is added to a message at the time the message is created.

Trojan Horse - A program or module that purports to perform a particular function but which secretly performs a different function (which may or may not include the purported function). Trojan Horse programs are widespread throughout the Internet.

Version Control - The method by which an evolving approved Gaming Platform is verified to be

Copyright © 2011 GLI Interactive BV All Rights Reserved.

operating in an approved state.

Copyright © 2011 GLI Interactive BV All Rights Reserved.

Appendix A: Submission Requirements

A.1 Introduction

A.1.1 General Statement. This chapter shall govern the types of information that are, or may be required to be submitted by the submitting party in order to have elements or components of an Interactive Gaming System tested to this Standard. Where the information has not been submitted or is not otherwise in the possession of the testing laboratory, the submitting party shall be asked to supply additional information. Failure to supply the information can result in denial in whole or in part of the submission and/or lead to testing delays.

A.1.2 Previous Submission. Where the testing laboratory has been previously supplied with the information on a prior submission, duplicate documentation is not required, provided that the previous information is referred to by the submitting party, and those documents are easily located at the testing laboratory. Every effort shall be made to reduce the redundancy of submission information.

A.2 Prototype (Full Submission) Submissions

A.2.1 General Statement. A Prototype (full submission) submission is a first time submission of a particular piece of hardware or software that has not previously been reviewed by the testing laboratory. For Modifications of previous submissions, including required changes to previously submitted Prototype (full submission) certification, whether certified or pending certification, see 'Submissions of Modifications (partial submissions) to a Previously Certified Item,' Section A.3.
NOTE: *Due to abnormal component complexity and/or excessive cost it is sometimes necessary for on-site testing of an Gaming Platform at the manufacturer's facility. The requirement for on-site testing will be assessed on a case-by-case basis.*

A.2.2 Submission Letter Requirements. Each submission shall include a request letter, on company letterhead, dated within one (1) week of the date the submission is received by the testing laboratory. The letter should include the following:

a) The jurisdiction(s) for which you are requesting certification;

Copyright © 2011 GLI Interactive BV All Rights Reserved.

b) The items requested for certification. In the case of software, the submitting party shall include ID numbers and revision levels, if applicable. In the case of proprietary hardware, the submitting party shall indicate the manufacturer, model, and part and revision numbers of the associated components of hardware; and

c) A contact person who will serve as the main point of contact for engineering questions raised during evaluation of the submission. This may be either the person who signed the letter or another specified contact.

A.2.3 Player Account Management Submission Requirements. The "Player Account Management" includes the components of the Gaming Platform which form the primary interface for the player. The Player Account Management interface provides the player with the means to register an account, log in / out of their account, modify their account information, deposit and withdraw funds to / from their account, request account activity statements / reports, and close their account. In addition, any web pages displayed to the player which relate to gaming, but which are not an actual game screen, are considered to be part of the Player Account Management components.

I. Source Code The following requirements apply to any Player Account Management component source code requested by the testing laboratory for evaluation:

a) Any Player Account Management component source code submitted to the testing laboratory shall be reviewed in a secure, controlled and supervised manner which is agreeable to the testing laboratory, the regulator and the software supplier;

b) Any Player Account Management component source code submitted to the testing laboratory shall contain the following information (at a minimum):

i. File / module / function name(s); and

ii. Brief description of the file / module / function purpose(s); and

c) Any Player Account Management component source code submitted to the testing laboratory shall be commented in an informative and useful manner.

II. Documentation The following documentation must be submitted for the evaluation of the Player Account Management components:

a) Detailed functional description of the Player Account Management components (including the gaming website home page and all gaming website peripheral pages);

Copyright © 2011 GLI Interactive BV All Rights Reserved.

b) Detailed descriptions of the following technical functionality available on the gaming platform:
    i. Player Account Registration,
    ii. Player Account Login (Username & Password),
    iii. Player Interface to Player Account,
    iv. Responsible Gaming Features,
    v. Privacy Policy, and
    vi. Player Account Deactivation.
c) Detailed description of how player verification information is protected from unauthorized access;
d) Detailed description of player authentication (i.e. how registered player identify themselves to the Gaming Platform each time they connect);
e) Description of how player registration and account information (including credit card information) is to be protected from unauthorized access;
f) Description of the register of unclaimed prize monies and how it is maintained; and
g) Description of the treatment of revenue from expired, unclaimed wins.

III. Test Environment – Supervised Build and Install Before commencing testing, the testing laboratory will supervise the build / compilation of the gaming platform source code into software. In this context, "supervise" means that a consultant from the testing laboratory must be present, in person or via a remote connection, while the gaming platform source code is being built / compiled.

The control-version(s) of the gaming platform, created as a result of the supervised build / compilation, must then be installed onto a suitable test environment. The testing laboratory and the software supplier must ensure that the software which is installed is the same version as was built / compiled under the testing laboratory's supervision. Particular attention will be given to any configuration made to the test environment to accommodate the software which has been installed. The testing laboratory must obtain a copy of any necessary configuration files.

The resulting test system must be similar to that of the production Gaming Platform, and identical in respect of all critical functionality in regard to the gaming platform, which

Copyright © 2011 GLI Interactive BV All Rights Reserved.

will enable meaningful testing of the software prior to it being loaded onto the live Gaming Platform.

Where an Gaming Platform requires the use of defined user roles, or accounts with associated passwords or PIN numbers, a default list of all users and passwords or PIN numbers must be submitted including a method to access the database.

A.2.4 ***Information Systems Security (ISS) Submission Requirements***. "ISS" refers to the physical, environmental, administrative and technical features implemented to maintain the security and integrity of the gaming environment. The following sections outline the submission requirements for an ISS evaluation.

I. **Documentation** The following documentation must be submitted for an ISS evaluation:

a) A copy of the Information Security Policy, including:

i) Details of the physical security processes implemented to protect the production gaming environment;

ii) Details of where and how each category of information (e.g. critical, important, not important) is stored in the Gaming Platform, and the risk assessment and protection measures implemented for each category of information;

iii) Details of the password protection systems and associated algorithms utilized by the Gaming Platform;

iv) Details of the method of transaction logging used;

v) Details of how self-monitoring is implemented;

vi) Details of the encryption methods used for the secure storage of critical information;

vii) Controls to prevent unauthorized use of operator consoles or accounts, and for the prevention of unauthorized access to information which may aid unauthorized access to the operator consoles or accounts (such as usernames, IP addresses or passwords);

viii) Details of the incident management system implemented by the operator;

ix) Details of the disaster recovery plan implemented by the operator;

x) Details of audit reports available from the Gaming Platform; and

Copyright © 2011 GLI Interactive BV All Rights Reserved.

xi) Reports showing how often the Information Security Policy is reviewed.

b) A general overview of the Gaming Platform design;

c) Details and functional specifications of all Gaming Platform components in the production environment including, but not limited to:

i) Platform Hardware, such as:

- Servers,
- Firewalls and Intrusion Detection Systems,
- Operator Consoles (local and remote),
- Gateways and Access Points,
- Remote Controllers,
- Remote Access Servers,
- Multiplexing Equipment,
- Switching Equipment,
- Monitoring Equipment,
- Hubs, Switches and Routers, and
- Repeaters.

ii) Operating Systems,

iii) Applications,

iv) Audit Subsystems, including any built-in functionality of the operating systems and applications used for audit purposes,

v) Duplication Strategy,

vi) Disk Subsystem, and

vii) Back-up facilities.

d) A network architecture diagram, including the following:

i) Network topology,

ii) Devices used to create the network,

iii) Internal and external IP addresses for all devices,

iv) Controls to prevent unauthorized modification to device configurations,

v) Local Area Network (LAN) and Virtual Local Area Network (VLAN) design, including all functional subnets and firewalls,

vi) Details of the gaming platform connections to the Internet, and

Copyright © 2011 GLI Interactive BV All Rights Reserved.

vii) Details of any remote connections (e.g. Internet, wide area network, dial-up) used to support Gaming Platform operations.

e) A list of all non-production systems (e.g. MIS) and third party systems that will connect to the Gaming Platform. For each external system provide:
   i) The connection method (e.g. dial-up, X.25, leased line, Internet).
   ii) Details of the information to be transferred in each direction.
   iii) The entity that initiates the information transfer.
   iv) The protocol used to perform the transfer.
   v) Controls to prevent access to other information on the Gaming Platform.
   vi) Controls to prevent unauthorized use of the connection.
   vii) Controls to prevent eavesdropping on communications between non-production systems and the Gaming Platform.

f) Details of any Network Management system associated with the internal production network, including:
   i) Physical location of the Network Management system.
   ii) Class of personnel authorized to use Network Management system.
   iii) Locations from where network management functions can be executed.
   iv) Network management protocol.
   v) The devices to be managed on a read only basis.
   vi) The devices to be managed on a read/write basis.
   vii) Controls to prevent unauthorized access to network management functions.
   viii) Controls to audit the use of network management functions.
   ix) Controls to detect unauthorized connections to the network.
   x) Controls to detect connection of unauthorized equipment to the network.
   xi) Describe the locations and physical and logical security arrangements associated with secondary DNS servers.

g) For the data encryption and communications between the Gaming Platform and the end player device, the following information must be supplied:
   i. Details of the message authentication algorithm used:
      - Description of the algorithm,
      - Theoretical basis of the algorithm,

Copyright © 2011 GLI Interactive BV All Rights Reserved.

- Results of any analyses or tests to demonstrate that the algorithm is suitable for the intended application,
- Rules for the selection of keys,
- Rules for changing keys,
- Means of generating and protecting keys.

ii. Details of the encryption to be used during game play, including:

- Encryption algorithm,
- Size of encryption keys,
- Key generation process,
- Key storage process,
- Key exchange procedure at session start-up,
- Subsequent key exchanges,
- Key revocation process in the event keys are compromised, and
- Details of any information that is not encrypted for transmission.

A.3 Submissions of Modifications (Partial Submissions) to a Previously Certified Item

A.3.1 ***General Statement*** For any update submission (e.g., a revision to existing hardware or software that is currently under review, certified or has been reviewed and not certified), the following information shall be required to process the submission in addition to the requirements set forth in 'Submission Letter Requirements'. All modifications require re-testing, examination, and re-certification by the testing laboratory.

NOTE: *Modifications to the supporting environment which do not impact the functionality of the component(s) under evaluation need not be resubmitted as these elements are not evaluated in our laboratory in the first place, and are only required to provide the supporting environment for the component under test. However, any environmental changes which in any way change the functionality of the component(s) under evaluation must be re-certified. Where there is some doubt over whether a Gaming Platform should be resubmitted then these situations will be considered on a case by case basis.*

Copyright © 2011 GLI Interactive BV All Rights Reserved.

A.3.2 ***<u>Hardware Re-Submission</u>***. Each hardware re-submission shall:

a) Identify the individual items being submitted (including part number);
b) Supply a complete set of schematics, diagrams, data sheets, etc. describing the modification along with the reason for the change(s); and
c) Provide the updated or new hardware, a description and the method of connection to the original Gaming Platform or hardware components.

A.3.3 ***<u>Player Account Management Re-Submission</u>***. Each Player Account Management component re-submission shall:

a) Use the same requirements as in the '*Player Account Management Submission Requirements*' listed above except where the documentation has not changed, in which case a resubmission of identical documents is not required.
b) Include a description of the software change(s) and modules affected;
c) Include updated functional specifications, where applicable; and
d) Include an updated source code package for the Gaming Platform, if applicable.

A.3.4 ***<u>Jackpot Re-Submission</u>***. Each jackpot re-submission shall:

a) Use the same requirements as in the '*Jackpot Submission Requirements*' listed above except where the documentation has not changed, in which case, a resubmission of identical documents is not required;
b) Include a description of the software change(s) and modules affected;
c) Include updated jackpot specifications; and
d) Include an updated source code package for the Gaming Platform.

A.3.5 ***<u>ISS Re-Submission</u>***. Each ISS re-submission shall:

a) Use the same requirements as in the '*Information Systems Security (ISS) Submission Requirements*' listed above except where the documentation has not changed, in which case a resubmission of identical documents is not required;
b) Include a detailed description of the Gaming Platform change(s) and component(s) affected, as well as the reason(s) for the changes implemented by the operator; and
c) Include updated ISS design and configuration documents where required.

Copyright © 2011 GLI Interactive BV All Rights Reserved.