GLI STANDARD SERIES

GLI-13:

STANDARDS FOR MONITORING AND CONTROL SYSTEMS AND VALIDATION SYSTEMS

VERSION: 3.0 DRAFT

REVISION DATE: APRIL 17, 2024

About This Standard

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

This document is intended to be used by regulatory bodies, operators, and industry suppliers as a compliance guideline for technologies and procedures pertaining to gaming. This standard is not intended to represent a set of prescriptive requirements that every Monitoring and Control System and Validation System and operator shall comply with; however, it does establish a standard regarding the technologies and procedures used to facilitate these operations.

Operators and suppliers are expected to provide internal control documentation, credentials, and associated access to a production equivalent test environment with a request that it be evaluated in accordance with this technical standard. Upon completion of testing, GLI will provide a certificate of compliance evidencing the certification to this Standard.

GLI-13 should be viewed as a living document that provides a level of guidance that will be tailored periodically to align with this developing industry over time as gaming implementations and operations evolve.

Table of Contents

Chapter 1: Introduction to Monitoring and Control Systems and Validation Systems

1.1 Introduction

1.1.1 General Statement

Gaming Laboratories International, LLC (GLI) has been testing Gaming Equipment since 1989. Over the years, GLI has developed numerous technical standards utilized by jurisdictions all over the world. This document, *GLI-13*, sets forth the technical standards for Monitoring and Control Systems and Validation Systems.

1.1.2 Document History

This document is a compilation based upon many standards documents from around the world. Some were written by GLI; others were written by industry regulators with input from independent test laboratories and gaming operators, developers, and suppliers. GLI has taken each of the standards documents and merged the unique rules, eliminated some rules and updated others, to reflect both the change in technology and the purpose of maintaining an objective standard that achieves common regulatory objectives without unnecessarily impeding technological innovation. GLI lists below, and gives credit to, agencies whose documents were reviewed prior to writing this Standard. It is the policy of GLI to update this document as often as warranted to reflect changes in technology and/or testing methods. This document will be distributed without charge and may be obtained by downloading it from the GLI website at www.gaminglabs.com or by contacting GLI at:

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

1.1.3 Acknowledgment of Other Standards Reviewed

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

1.2 Purpose of Technical Standards

1.2.1 General Statement

The purpose of this technical standard is as follows:

a) To eliminate subjective criteria in the evaluation and certification of Monitoring and Control Systems and Validation Systems.

b) To assess the criteria that impacts the credibility and integrity of gaming from both revenue collection and player perspectives.
c) To establish a standard that will ensure gaming is fair, secure, auditable, and able to be operated correctly.
d) To distinguish between local public policies and Independent Test Laboratory criteria, acknowledging that it is the prerogative of each regulatory body to set its own public policies with respect to gaming.
e) To recognize that the evaluation of internal controls (such as anti-money laundering, financial, and business processes) employed by operators should not be incorporated into the laboratory testing of the standard. Instead, these should be addressed within operational audits performed for local jurisdictions.
f) To develop a standard that can be easily revised to allow for new technology.
g) To formulate a standard that does not specify any particular design, method, or algorithm, thereby allowing a wide range of methods to conform to the standards while simultaneously encouraging the development of new methods.

1.2.2 No Limitation of Technology

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

1.2.3 Adoption and Observance

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

1.3 Other Documents That May Apply

1.3.1 Other GLI Standards

This technical standard covers the requirements for Monitoring and Control Systems and Validation Systems. Depending on the technology utilized by a system, additional GLI technical standards may also apply.

NOTE: The entire family of GLI Standards is available free of charge at www.gaminglabs.com.

1.3.2 Minimum Internal Control Standards (MICS)

Implementing Monitoring and Control Systems and Validation Systems is a complex endeavor, necessitating the development of internal processes and procedures to ensure the gaming environment is secure and controlled adequately. To that end, it is expected that a set of Minimum Internal Control Standards (MICS) will be established to define the internal processes for the

management and handling of gaming as well as the requirements for internal control of any system or component software and hardware, and their associated accounts.

1.3.3 Gaming Security Framework (GSF)

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

NOTE: The GLI Gaming Security Framework is available free of charge at www.gaminglabs.com. *[To be released for comment in the near future]*

1.4 Interpretation of this Document

1.4.1 General Statement

This technical standard applies to Gaming Systems that:

a) For Monitoring and Control Systems, monitor and control Gaming Equipment by providing logging, searching, and reporting of significant events, collection of individual financial and meter data, reconciliation of meter data against counts, and control and configuration of supported Gaming Equipment within the Gaming Venue:
b) For Validations Systems, securely maintain records of wagering instruments (vouchers and/or coupons), validate payment of wagering instruments, record successful or failed payments of wagering instruments, and control the purging of expired wagering instruments.

NOTE: When referenced within this document, the term "Gaming Systems" refers to Monitoring and Control Systems and Validations Systems, and the term "Gaming Equipment" refers to any gaming device, electronic table game, electronic wager station, live game management component, kiosk, or any other critical electronic gaming component and its interface element intended for use with such systems,
NOTE: This document is not intended to define which parties are responsible for meeting the requirements detailed herein. It is the responsibility of the stakeholders of each jurisdiction to determine how to best meet the requirements laid out in this document.

1.4.2 Software Suppliers and Operators

The components of a gaming environment, although they may be constructed in a modular fashion, are intended to function cohesively.

a) Monitoring and Control Systems and Validation Systems may be developed to have configurable features; the final configuration of which depends on the options chosen by the operator. From a testing perspective, it might not be possible to test all of the configurable features of a gaming environment submitted by a software supplier in the absence of the final configuration chosen by the operator; however, the configuration that will be utilized in the production environment

shall be communicated to the independent test laboratory to facilitate creating a functionally equivalent test environment.

b) Because of the integrated nature of a gaming environment, there are several requirements in this document which may apply to both operators and suppliers. In such cases, the collection of systems and solutions needed to meet these requirements will be considered to be the gaming environment and the individual entities providing them will need to meet such eligibility requirements as the regulatory bodies deem appropriate for performance of these requirements.

1.5 Testing and Auditing

1.5.1 Laboratory Testing

The independent test laboratory will test and certify the components of the Monitoring and Control Systems and Validation Systems in accordance with the chapters of this technical standard within a controlled test environment, where applicable. Requirements necessitating additional operational procedures for compliance will be documented in the evaluation report to augment the operational audit's scope.

NOTE: Upon request, or as required by the regulatory body, the independent test laboratory will conduct on-site testing where the Gaming System, Gaming Equipment, and communications are set-up and tested within the Gaming Venue prior to implementation.

1.5.2 Operational Audits

The integrity and accuracy of the operation of Monitoring and Control Systems and Validation Systems is highly dependent upon operational procedures, configurations, and the production environment's network infrastructure. In addition to the testing and certification of Monitoring and Control System and Validation System components, a regulatory body may elect to require the following operational audits be conducted on a periodic basis:

a) An internal controls audit, using the recommended scope outlined within the appendix of this document for "Internal Controls for Gaming Venues"; and/or
b) A technical security controls audit, against the controls identified in the GLI Gaming Security Framework (GLI-GSF).

Chapter 2: General Gaming System Requirements

2.1 Introduction

2.1.1 General Statement

The requirements throughout this chapter apply to Gaming Systems which may include Monitoring and Control Systems and/or Validation Systems. If the Gaming System is comprised of multiple computer systems at various sites, the system as a whole and all communication between its components shall conform to the applicable technical requirements within this document.

2.2 System Clock Requirements

2.2.1 System Clock

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

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

2.2.2 Time Synchronization

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

2.3 Control Program Requirements

2.3.1 Control Program Self-Verification

The Gaming System shall be capable of verifying that all critical control program components contained on the system are authentic copies of the approved components of the system on demand using a method approved by the regulatory body. The critical control program authentication mechanism shall:

a) Employ a cryptographic hash algorithm which produces a message digest of at least 128 bits. Other test methodologies shall be reviewed on a case-by-case basis;
b) Include all critical control program components which may affect gaming operations, including but not limited to executables, libraries, gaming or system configurations, operating system files, components that control required system reporting, and database elements that affect system operations; and
c) Provide an indication of the authentication failure if any critical control program component is determined to be invalid.

2.3.2 Control Program Independent Verification

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

2.4 Critical Components and Functions

2.4.1 Communications

The communication techniques used by the Gaming System shall have proper error detection and recovery mechanisms, which are designed to prevent intrusion, interference, eavesdropping and tampering. Any alternative implementations will be reviewed on a case-by-case basis.

a) All data transmitted between critical components shall utilize an appropriate level of cryptography for the information being transmitted.
b) The communication process used by the critical components shall be:
   i. Robust and stable enough to secure each transmission such that failure event(s) can be identified and logged for subsequent audit and reconciliation; and
   ii. Protected against the capture of authentication data transmitted during the authentication and against manipulation by unauthorized parties.
c) If communications between critical components are lost, the affected components shall cease operations related to that communication. It is permissible for this error to be detected when the critical components try to communicate with one another.

2.4.2 Servers and Databases

The Gaming System may include one or more servers, part of a networked or distributed system, which manages the overall operations of the Gaming System, along with associated databases that archive all input and collected data. These requirements apply not only to the system's front end but also to any underlying database. Each database must maintain a user audit trail that is safeguarded against unauthorized access, ensuring the integrity and security of data across all levels of the system.

2.4.3 Front-End Processor and Data Collectors

The Gaming System may possess a Front-End Processor that gathers and relays all data from the connected Data Collectors to the associated databases. The Data Collectors, in turn, collect all data from connected Gaming Equipment.

a) If the Front-End Processor maintains buffered/logging information, a secure mechanism shall be in place which prevents the loss of critical data contained herein.
b) All received data shall be stored on the databases before the Monitoring and Control System may purge data from the Front-End Processor, the connected Data Collectors, and the connected Gaming Equipment.

2.4.4 Workstations

For workstations used to perform regulated functions of the Gaming System, access by an individual shall be controlled by a secure logon procedure or other secure process approved by the regulatory body to ensure that only authorized personnel are allowed access. It shall not be possible to modify the configuration settings of the Gaming System without an authorized secure process. The following additional requirements apply when user sessions are supported by the workstation:

a) A user session, where supported by workstations, is initiated by the individual logging in to their user account using their secure username and password or an alternative means for the individual to provide authentication credentials as allowed by the regulatory body.
b) All available options presented to the individual shall be tied to their user account.
c) If the workstation does not receive input from the individual within five minutes, or a period specified by the regulatory body, the user session shall time out or lock up, requiring the individual to re-establish their login in order to continue.

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

2.4.5 Gaming Equipment Identification

The Gaming System must uniquely identify each connected instance of Gaming Equipment. This unique identification number shall be utilized by the Gaming System to log and track all essential information pertaining to the corresponding Gaming Equipment. Furthermore, the system must prevent the duplication of these identification numbers to ensure the integrity and accuracy of the equipment tracking.

2.4.6 Communication Loss Alerts

The Gaming System shall generate alerts for communication loss with any Gaming Equipment. It is permissible for the Gaming System to detect this error when the system tries to communicate with the Gaming Equipment.

2.5 Information to be Maintained

2.5.1 Data Retention and Time Stamping

The Gaming System shall be capable of maintaining and backing up all applicable recorded data as discussed within this section, unless properly communicated to another Gaming System, which will assume these responsibilities:

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

2.5.2 System Significant Event Information

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

a) Failed user account access attempts, including IP Address;
b) Program error or authentication mismatch;
c) Significant periods of unavailability of any critical component of the system (e.g., communications are halted and/or system functions cannot be successfully completed for any user);
d) System voids, overrides, and corrections;
e) Changes to live data files occurring outside of normal program and operating system execution;
f) Changes that are made to the download data library, including the addition, changing or deletion of software, where supported;
g) Changes to policies and parameters for operating systems, databases, networks, and applications (e.g., audit settings, password complexity settings, system security levels, manual updates to databases, etc.);
h) Changes to date/time on master time server;
i) Irrecoverable loss of sensitive information;
j) Any other activity requiring user intervention and occurring outside of the normal scope of system operation; and
k) Other significant or unusual events as deemed applicable by the regulatory body.

2.5.3 User Account Information

For Gaming Systems which support user account management, the information to be maintained and backed up for each user account shall include, as applicable:

a) Unique user account ID and username (if different);
b) User's name and title or position;
c) Full list and description of functions that each group or user account may execute;
d) The date and time the account was created;
e) The date and time of last access, including IP Address;;
f) The date and time of last password change;
g) The date and time the account was disabled/deactivated;
h) Group membership of user account; and
i) The current status of the user account (e.g., active, inactive, closed, suspended, etc.).

2.6 Reporting Requirements

2.6.1 General Reporting Requirements

The Gaming System shall be capable of providing the necessary information to produce reports as required by the regulatory body, unless properly communicated to another Gaming System, which will assume these responsibilities. In addition to meeting the requirements in the section above for "Data Retention and Time Stamping", the following requirements shall apply for required reports:

a) These required reports shall be able to be produced on demand, on a daily basis, and for other

intervals required by the regulatory body (e.g., month-to-date (MTD), year-to-date (YTD), life-to-date (LTD), etc.).

b) Each required report shall contain:
   i. The operator's name (or other identifier), the title of report, the selected interval and the date/time the report was generated;
   ii. An indication of "No Activity" or similar message if no information appears for the period specified; and
   iii. Labeled fields which can be clearly understood in accordance with their function.

2.6.2 System Significant Events and Alterations Reports

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

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

Chapter 3: Monitoring and Control System Requirements

3.1 Introduction

3.1.1 General Statement

The requirements of this chapter apply for the functionality of a Monitoring and Control System within a Gaming Venue. This section does not govern advanced bi-directional communication protocols (i.e., EFT, AFT, Bonusing, Promotional, System Based Progressives, features that utilize an RNG, etc.) that support credit transfers between Gaming Equipment and Gaming Systems.

3.2 Handpay Slip Requirements

3.2.1 Handpay Slips Generation

Where supported, a Monitoring and Control System shall have an application or facility that captures and processes every handpay message from Gaming Equipment or attendant intervention as needed, including for the payout of attendant paid awards and cancelled credits. Once captured, there shall be adequate access controls to allow for authorization, alteration, or deletion of any of the values prior to payment or execution.

NOTE: Where required by the regulatory body, if an attendant paid award is in excess of any taxation limit that is defined or configured for the game or feature, the attendant shall be advised of the needed to report taxable winnings to the proper authorities. When a mechanism is used to return taxable winnings to the Gaming Equipment, user intervention is required to void the original handpay slip that is generated.

3.2.2 Handpay Slip Information

The following information is required for all handpay slips generated with some or all fields to be completed by the Monitoring and Control System:

a) The type of slip (e.g., attendant paid awards, cancelled credits, short pay, special pay, etc.);
b) Slip sequence number which, for a printed slip, may be preprinted or concurrently-printed;
c) The date and time (shift if required);
d) Unique Gaming Equipment ID or equivalent;
e) Amount of payout in local monetary units, or description of merchandise prize awarded;
f) For attendant paid awards, as applicable:
    i. The amount wagered by the player and game outcome;
    ii. An indication advising the need for taxable winnings to be reported to the proper authorities, where required by the regulatory body;
    iii. Total before taxes and taxes withheld;
    iv. Additional payout information;
    v. The amount paid to the player, if different than the amount of payout;
g) Readings of metering information; and
h) Relevant physical or electronic signatures required by the regulatory body.

3.3 Fill/Credit Slip Requirements

3.3.1 Fill/Credit Slips Generation

Where supported, a Monitoring and Control System shall have an application or facility that captures and processes fills and credits for Gaming Equipment as needed. Once captured, there shall be adequate access controls to allow for authorization, alteration, or deletion of any of the values prior to payment or execution.

3.3.2 Fill/Credit Slip Information

The following information is required for all fill/credit slips generated with some or all fields to be completed by the Monitoring and Control System:

a) The type of slip (e.g., fill, credit, etc.);
b) Slip sequence number which, for a printed slip, may be preprinted or concurrently-printed;
c) The date and time (shift if required);
d) Unique Gaming Equipment ID or equivalent;
e) Amount of fill or credit by denomination and in total;
f) Readings of metering information; and
g) Relevant physical or electronic signatures required by the regulatory body.

3.4 Gaming Equipment Management

3.4.1 General Statement

The requirements of this section shall be met by the Gaming Equipment either directly or through the use of an interface element which meets the "Interface Element Requirements" chapter of this document.

3.4.2 Gaming Equipment Asset Registry (GEAR)

The Monitoring and Control System shall include a Gaming Equipment Asset Registry (GEAR), which maintains the following in a searchable database for each Gaming Equipment in operation, as applicable:

a) Unique interface element or asset ID;
b) Unique Gaming Equipment ID or description (e.g. serial number, manufacturer);
c) The date and time the Gaming Equipment was made available for use;
d) For Multi-Venue Monitoring and Control Systems, Gaming Venue Name/Site Identifier;
e) Gaming Equipment location description;
f) The type of Gaming Equipment (gaming device, kiosk, etc.);
g) Equipment configuration data (e.g., peripherals, communications, progressive jackpots, etc.);
h) For electronic games:
    i. Game configuration data (e.g., game themes, paytables, denominations, etc.);

ii. Theoretical return to player (RTP) for each game theme/paytable;
i) Significant event information;
j) Metering information;
k) Critical control programs installed;
l) The current status of the Gaming Equipment (active, disabled, decommissioned, etc.); and
m) The date and time the Gaming Equipment was or is scheduled to be decommissioned (blank until known).

NOTE: If the Monitoring and Control System retrieves any of these parameters directly from the Gaming Equipment, sufficient controls shall be in place to ensure accuracy of the information in the GEAR.

3.4.3 Significant Events and Metering Information

The following applicable Gaming Equipment information shall be correctly communicated to the Monitoring and Control System for storage according to the secure communication protocol implemented:

a) Significant event information, as defined within the *GLI-11 Standards for Gaming Devices* and/or other applicable jurisdictional requirements observed by the regulatory body, which includes the following for each significant event:
   i. The date and time which the event occurred;
   ii. Unique Gaming Equipment ID that generated the event;
   iii. A unique number/code that defines the event; and
   iv. A brief text that describes the event in the local language.
b) Metering information, as defined within the *GLI-11 Standards for Gaming Devices* and/or other applicable jurisdictional requirements observed by the regulatory body, in local monetary units. Meters shall be labeled so they can be clearly understood in accordance with their function.

NOTE: This information may be either read directly from the Gaming Equipment or relayed using a delta function. It is acceptable to use secondary system calculations where appropriate.

3.4.4 Machine Entry Authorization Log (MEAL)

When the ability to automatically record entry to Gaming Equipment is supported, the Machine Entry Authorization Log (MEAL) shall contain, at a minimum, the following, where supported:

a) Unique Gaming Equipment ID being entered;
b) Identification of individual who entered the Gaming Equipment;
c) The date and time of entry;
d) The duration of entry;
e) The reason for entry; and
f) Activity while entered, including the specific areas accessed and changes made.

NOTE: Entries in the MEAL are not required when removing a stacker or drop box from Gaming Equipment during normal drop procedures.

3.5 Monitoring and Control System Reports

3.5.1 General Statement

In addition to meeting the "General Reporting Requirements", the Monitoring and Control System shall be capable of providing the necessary information to produce the reports listed in this section as required by the regulatory body, unless properly communicated to another Gaming System, which will assume these responsibilities.

3.5.2 Comparison Reports

The following comparison reports shall be able to be produced for each Gaming Equipment, as applicable:

a) Metered vs. Actual Handpay Comparison Reports. These reports are to include, for each type of handpay (e.g., attendant paid awards, cancelled credits, etc.) and aggregate, comparisons of metered amounts to actual amounts with the currency and percentage variances;
b) Metered vs. Actual Drop Comparison Reports. These reports are to include, for each medium dropped (e.g., bills, vouchers, coupons, etc.) and aggregate, comparisons of metered amounts to actual amounts with the currency and percentage variances; and
c) Theoretical vs. Actual RTP Percentage Comparison Reports. These reports are to include, for each game theme/paytable, comparisons of the configured theoretical RTP percentage to the actual RTP percentage with percentage variances.

NOTE: It is acceptable to combine reporting data where appropriate (e.g., revenue, theoretical/actual comparison).

3.5.3 Game Performance Reports

The following information shall be provided to produce one or more reports on game performance for each Gaming Equipment, as applicable:

a) Unique Gaming Equipment ID or equivalent;
b) The date and time the Gaming Equipment was made available for play;
c) The name of each game theme and game type (reel game, live table game, etc.);
d) For each game theme/paytable and in total:
    i. Theoretical RTP percentage;
    ii. Actual RTP percentage;
    iii. The number of games played;
    iv. Amounts wagered;
    v. Amounts won; and
e) The current status of the Gaming Equipment (active, disabled, decommissioned, etc.).

Chapter 4: Validation System Requirements

4.1 Introduction

4.1.1 General Statement

A Validation System may be entirely integrated into another system or exist as an entirely separate Gaming System. Validation Systems are generally classified into two types: bi-directional Validation Systems that allow Gaming Equipment to issue and redeem wagering instruments (TITO) and wagering instrument out only Validation Systems that allow Gaming Equipment to issue wagering instruments but do not allow wagering instrument redemption. This chapter primarily addresses bi-directional Validation Systems. Where wagering instrument out only systems are utilized, some of this chapter may not apply.

4.2 Wagering Instruments

4.2.1 Wagering Instrument Communications

The Validation System shall process wagering instrument transactions correctly according to the secure communication protocol implemented.

4.2.2 Wagering Instrument Information

A wagering instrument shall contain the following information at a minimum:

a) The date and time of issuance;
b) Numeric value of the wagering instrument;
c) Unique validation number (and which for a printed wagering instrument, shall appear on the leading edge of the wagering instrument);
d) Barcode or any machine-readable code representing the unique validation number;
e) Unique Gaming Equipment ID or equivalent which issued the wagering instrument;
f) The type of wagering instrument or other method of differentiating wagering instrument types, assuming multiple types are available. Additionally, it is strongly recommended that whenever the wagering instrument type is itself a non-cashable coupon and/or just a receipt, that the wagering instrument explicitly states that it has “no cash value” or other equivalent wording;
g) For a printed wagering instrument, it is permissible for the following information to be contained on the ticket stock itself:
    i. Gaming Venue Name/Site Identifier; and
    ii. Indication of an expiration period from date of issue, or date the wagering instrument will expire;
    i. Indication if the wagering instrument is a “duplicate”, assuming duplicate wagering instruments may be printed;
h) For a printed wagering instrument which can be redeemed without attendant intervention, the following additional information shall also be printed:
    i. Alpha value of the wagering instrument; and

ii. Wagering instrument sequence number, which may be preprinted or concurrently-printed.

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

4.2.3 Wagering Instrument Records

For each wagering instrument, the Validation System shall maintain the following information in a searchable database, as applicable:

a) Unique validation number;
b) The date and time of issuance;
c) Value of the wagering instrument;
d) Unique Gaming Equipment ID or equivalent which issued the wagering instrument;
e) For Multi-Venue Validation Systems, Gaming Venue Name/Site Identifier where issuance occurred;
f) The type of wagering instrument or other method of differentiating wagering instrument types, assuming multiple types are available;
g) Indication of an expiration period from date of issue, or date the wagering instrument will expire;
h) For a redeemed wagering instrument (blank until known):
   i. The date and time of redemption;
   ii. Unique Gaming Equipment ID or equivalent which redeemed the wagering instrument;
   iii. For Multi-Venue Validation Systems, Gaming Venue Name/Site Identifier where redemption occurred;
i) For a voided wagering instrument (blank until known):
   i. The date and time of voiding;
   ii. Unique Gaming Equipment ID or equivalent which voided the wagering instrument;
   iii. For Multi-Venue Validation Systems, Gaming Venue Name/Site Identifier where voiding occurred;
j) For an expired wagering instrument, the date and time of expiration (blank until known); and
k) The current status of the wagering instrument (i.e., valid, unredeemed, pending, void, invalid, redemption in progress, redeemed, expired, etc.).

4.3 Wagering Instrument Issuance

4.3.1 Wagering Instrument Issuance

The Gaming Equipment may pay the player by issuing a printed or virtual wagering instrument that contains the information as indicated in the section entitled “Wagering Instrument Information” above. Payment by wagering instrument is only permissible when:

a) The Gaming Equipment is linked to a Validation System which allows for the validation of the wagering instrument. Provisions shall be made if communication is lost and validation information cannot be sent to the Validation System, thereby requiring the manufacturer to support some alternate method of payment; or

b) Utilizing an approved alternative method that includes the ability to identify duplicate wagering instruments to prevent fraud through the redemption of a wagering instrument that was previously issued by the Gaming Equipment.

4.3.2 Wagering Instrument Issuance Limits

Payment by wagering instruments where the amounts being paid exceed a Gaming Equipment or System configured limit (i.e. the credit limit, transaction limit, etc.) shall result in a handpay lockup or tilt on the Gaming Equipment.

4.3.3 Online Wagering Instrument Issuance

The Validation System and Gaming Equipment shall support the bi-directional transmission of the following information when issuing a wagering instrument, as applicable:

a) The date and time of issuance;
b) Value of the wagering instrument;
c) Unique validation number;
d) Unique Gaming Equipment ID or equivalent which issued the wagering instrument;
e) Gaming Venue Name/Site Identifier; and
f) Indication of an expiration period from date of issue, or date the wagering instrument will expire.

4.3.4 Validation Number Generation

The wagering instrument's unique validation number shall be generated by the Validation System or the Gaming Equipment:

a) Validation System Generated. The algorithm or method used by the Validation System to generate the unique validation number shall guarantee an insignificant percentage of repetitive validation numbers.
b) Gaming Equipment Generated. The Validation System shall send a unique seed to the Gaming Equipment upon enrolling the Gaming Equipment as wagering instrument capable. The system may subsequently send a new seed to the Gaming Equipment after a wagering instrument is issued. The algorithm or methods used to determine the seed shall guarantee an insignificant percentage of repetitive validation numbers.

4.3.5 Wagering Instrument Issuance During Communication Loss

Unless the Validation System and Gaming Equipment support offline wagering instrument issuance, the following requirements shall be met:

a) When using a non-seeded method, if any links between the Gaming Equipment and the Validation System go down, the Gaming Equipment shall:
   i. Not respond to the validation request and stop wagering instrument issuance;
   ii. Prevent further issuance of wagering instruments; or

iii. Not read or store any further wagering instrument information generated by the Gaming Equipment.

b) In cases where the Gaming Equipment has already been 'seeded' by the Validation System, a maximum of two wagering instruments directly after loss of communication is acceptable, provided the wagering instrument issuance information is sent immediately, when communication is reestablished.

4.3.6 Offline Wagering Instrument Issuance

For the support of offline wagering instrument issuance, the Gaming Equipment shall be linked to an approved Validation System that allows validation of the wagering instrument but does not have to be in constant communication for the issuance of wagering instrument to be permissible. The following requirements shall be met to support the issuance of offline wagering instruments after a loss of communication with the Validation System has been identified:

a) The Gaming Equipment shall not issue more offline wagering instruments than it has the ability to store locally.
b) The Gaming Equipment shall not request validation numbers, or values for seeds, keys, etc. used in the issuance of wagering instruments, until all outstanding offline wagering instrument information has been fully communicated to the Validation System.
c) The Gaming Equipment shall request a new set of validation numbers, seeds, keys, etc. if the current list has the possibility of being compromised.
d) The complete validation numbers, or values for the seeds, keys, etc. shall never be viewable through any display supported by the Gaming Equipment.
e) The Validation System shall be able to set an expiration length for all provided and still unused validation numbers and seed, key, etc. values. Expired validation numbers and seed, key, etc. values shall be discarded in a way that prevents the re-use of unique combinations of validation numbers and seed, key, etc. values for a sufficient period of time on the system.
    i. Secure seeds, keys, etc. as assigned shall be sufficiently random. Measures to avoid predictability will be reviewed by the independent test laboratory on a case-by-case basis.
    ii. The minimum length for any secure seeds, keys, etc. employed by the Validation System shall be chosen from a pool of the variable type specified by the communication protocol utilized. The pool shall be comprised of at least 10 to the power of 14 randomly distributed values.
f) An "offline authentication identifier" shall be included on the wagering instrument.
    i. For printed wagering instruments, this identifier shall appear on the next line immediately following the leading-edge validation number that in no way overwrites, or otherwise compromises, the printing of the validation number on the wagering instrument (not required for wagering instruments that are non-redeemable without attendant intervention).
    ii. For cases where a suitable authentication identifier is not included on the wagering instrument, the Gaming Equipment shall issue at most one wagering instrument after the communications between the Gaming Equipment and the system have been lost.
g) The offline authentication identifier shall be derived by a hash algorithm, or other secure cryptographic method of at least 128 bits, that will uniquely identify the wagering instrument, verify that the redeeming system was also the issuing system, and validate the amount of the wagering instrument. The following minimum set of inputs shall be used to create the offline authentication identifier:

i. Unique Gaming Equipment ID or equivalent;
ii. Unique validation number;
iii. Value of the wagering instrument; and
iv. Secure seed, key, etc. provided by the Validation System to the Gaming Equipment.

4.4 Wagering Instrument Redemption

4.4.1 Wagering Instrument Redemption Process

The Validation System shall update the wagering instrument status on the database during each phase of the redemption process accordingly. In other words, whenever the wagering instrument status changes, the system shall update the database. Upon each status change, the database shall indicate the following information:

a) Unique validation number;
b) Value of the wagering instrument;
c) The date and time of status change; and
d) The current status of the wagering instrument (i.e., valid, unredeemed, pending, void, invalid, redemption in progress, redeemed, etc.).

4.4.2 Wagering Instrument Redemption Limits

If a player redeems a wagering instrument and that redemption would exceed Gaming Equipment or System configured limits (i.e. the credit limit, transaction limit, etc.) then this wagering instrument may only be redeemed provided that the player is clearly notified that they have redeemed less than requested to avoid player disputes, and the Gaming Equipment issues a wagering instrument that reflects the remaining credits.

4.4.3 Online Wagering Instrument Redemption

Wagering instruments can be redeemed at any Gaming Equipment which is enrolled for wagering instrument validation with a Validation System provided that no credits are issued to the Gaming Equipment prior to confirmation of wagering instrument validity.

4.4.4 Offline Wagering Instrument Redemption

If supported, offline wagering instruments can be redeemed at Cashier Station provided they are enrolled for wagering instrument validation with a Validation System and the identification and redemption of offline wagering instruments are supported through a system provided application.

4.5 Cashier Station Operation

4.5.1 Cashier Wagering Instrument Redemption

When wagering instruments are presented for redemption at a Cashier Station, the cashier shall scan the barcode (via a barcode reader or equivalent) or manually input the validation number and perform a verification with the Validation System.

4.5.2 Invalid Wagering Instrument Notification

The Validation System shall have the ability to identify and provide a notification to the Cashier Station in the case of invalid or unredeemable wagering instrument for the following conditions:

a) Wagering instrument cannot be found on file or has expired;
b) Wagering instrument has already been paid or voided; or
c) The value of wagering instrument differs from amount on file. This requirement can be met by display of wagering instrument for confirmation by the Cashier Station during the redemption process.

4.5.3 Wagering Instrument Redemption Receipt

The Cashier Station may issue a redemption receipt, after the wagering instrument is electronically validated, if applicable. If printed, the redemption receipt, at a minimum, shall contain the following information:

a) Unique Gaming Equipment ID or equivalent which issued the wagering instrument;
b) Unique validation number;
c) The date and time of redemption;
d) Value of the wagering instrument; and
e) Unique Cashier Station ID or user account ID which redeemed the wagering instrument.

4.6 Wagering Instrument Meters and Logs

4.6.1 Information Access

The wagering instrument meters and transaction logs required by this section shall have the ability to be displayed on demand using an authorized access method to ensure that only authorized personnel are allowed access. The meters and logs may be maintained locally by the Gaming Equipment and/or by an external critical component which records these meters and logs.

4.6.2 Wagering Instrument Meters

Electronic accounting meters shall be at least ten (10) digits in length. Eight (8) digits shall be used for the integer currency (e.g., dollar) amount and two (2) digits used for the sub-currency (e.g., cents) amount. The meters shall automatically roll over to zero once its maximum logical value has been reached. Meters shall be labeled so they can be clearly understood in accordance with their function.

a) The required electronic accounting meters for each Gaming Equipment are as follows:
   i. Voucher In. There shall be a meter that accumulates the total value of all wagering vouchers accepted by the Gaming Equipment;

ii. Voucher Out. There shall be a meter that accumulates the total value of all wagering vouchers issued by the Gaming Equipment;
iii. Coupon Promotion In. There shall be a meter that accumulates the total value of all promotional coupons accepted by the Gaming Equipment;
iv. Coupon Promotion Out. There shall be a meter that accumulates the total value of all promotional coupons issued by the Gaming Equipment; and
v. Other Meters. Wagering instrument transactions that would not otherwise be metered under any of the above meters, shall be recorded on sufficient meters to properly reconcile all such transactions.

b) The operation of other mandatory meters for Gaming Equipment shall not be impacted directly by wagering instrument transactions.

NOTE: Any accounting meter that is not supported by the functionality of the Gaming Equipment is not required to be implemented by the supplier.

4.6.3 Wagering Instrument Transaction Log

There shall be the capacity to display a complete transaction log for the previous thirty-five (35) transactions that incremented any of the "Wagering Instrument Meters". The following information shall be displayed:

a) The type of transaction (issuance/redemption);
b) The type of wagering instrument or other method of differentiating wagering instrument types, assuming multiple types are available;
c) The transaction value in local monetary units in numerical form;
d) The time of day of the transaction, in twenty-four (24) hour format showing hours and minutes;
e) The date of the transaction, in any recognized format, indicating the day, month, and year; and
f) Unique validation number where, for wagering instruments that have yet to be redeemed, only the last four (4) digits may be displayed by the Gaming Equipment.

NOTE: It is acceptable to have wagering instrument transactions recorded in separate logs or in a larger log which also contains records of other types of transactions (e.g. cashless transactions, bonusing transactions, promotional transactions, etc.).

4.7 Validation System Reports

4.7.1 General Statement

In addition to meeting the "General Reporting Requirements", the Validation System shall be capable of providing the necessary information to produce the reports listed in this section as required by the regulatory body, unless properly communicated to another Gaming System, which will assume these responsibilities.

4.7.2 Wagering Instrument Reports

The following reports shall be able to be produced for the reconciliation of wagering instruments:

a) Wagering Instrument Issuance Reports. These reports are to include, for each issued wagering instrument, the date and time of issuance, value, validation number, Gaming Equipment ID or equivalent which issued the wagering instrument;
b) Wagering Instrument Redemption Reports. These reports are to include, for each redeemed wagering instrument, the date and time of issuance, value, validation number, Gaming Equipment ID or equivalent which issued the wagering instrument, and date and time of redemption, and Gaming Equipment ID or equivalent which redeemed the wagering instrument;
c) Wagering Instrument Liability Reports. These reports are to include, for each unredeemed wagering instrument, the date and time of issuance, value, validation number, Gaming Equipment ID or equivalent which issued the wagering instrument, and date and time of expiration;
d) Wagering Instrument Expiration Reports. These reports are to include, for each expired wagering instrument, the date and time of issuance, value, validation number, Gaming Equipment ID or equivalent which issued the wagering instrument, and date and time of expiration; and
e) Wagering Instrument Void Reports. These reports are to include, for each voided wagering instrument, the date and time of issuance, value, validation number, Gaming Equipment ID or equivalent which issued the wagering instrument, and date and time of voiding.

4.7.3 Meter Reconciliation Reports

The following information shall be provided to produce one or more reports for reconciling each Gaming Equipment's metered amounts against the Validation System's recorded amounts, as applicable:

a) Unique Gaming Equipment ID or equivalent;
b) Voucher In meter vs. system recorded voucher redemptions;
c) Voucher Out meter vs. vouchers system recorded voucher issuances;
d) Coupon Promotion In meter vs. system recorded coupon redemptions;
e) Coupon Promotion Out meter vs. system recorded coupon issuances; and
f) Any other information needed for reconciliation which is not covered by the above.

4.7.4 Cashier Summary and Detail Reports

The following information shall be provided to produce one or more reports for each cashier session:

a) Unique Cashier Station ID or equivalent;
b) User account ID or name of cashier;
c) The date and time the cashier session began;
d) The cashier balances at the start and end of the cashier session;
e) For each wagering instrument transaction:
    i. Unique transaction ID;
    ii. The type of transaction (e.g., issuance, redemption, void, etc.);
    iii. The type of wagering instrument or other method of differentiating wagering instrument types, assuming multiple types are available;
    iv. The transaction value in local monetary units in numerical form;
    v. The date and time of the transaction; and

f) The cashier balance at the end of the cashier session (blank until known).

Chapter 5: Interface Element Requirements

5.1 Introduction

5.1.1 General Statement

An interface element is a device or facility which may be used to connect Gaming Equipment to the Gaming System for the purposes of communications relevant to that system.

5.2 Interface Hardware Requirements

5.2.1 General Statement

All proprietary interface element hardware shall meet the applicable requirements within this section. Unless otherwise directed by the regulatory body, these requirements do not apply to interface element hardware that solely utilizes unaltered commercial off-the-shelf (COTS) components, such as a PC or a display/monitor. For interface element hardware that utilize modified off-the-shelf (MOTS) components, these requirements will apply only to the modifications made to the components.

5.2.2 Player Safety and Environmental Effects on Integrity

The following requirements only apply to any interface element hardware which has locally stored critical non-volatile (NV) memory and/or installed software which has the potential to influence the regulated operations of the Gaming Equipment.

a) Electrical and mechanical parts and design principles of the interface element hardware shall not subject a player to any physical hazards.
b) The interface element shall be impervious to influences from Electro-Static Discharge (ESD). Protection against ESD requires that the interface element hardware be earthed in such a way that static discharge energy shall not permanently damage or permanently impact the normal operation of the electronics or other components within interface element. An interface element may exhibit temporary disruption when subjected to a significant external ESD with a severity level of 8kV air discharge and 4kV contact discharge. The interface element shall exhibit a capacity to recover and complete any interrupted operation without loss or corruption of any locally stored control information or critical data following any temporary disruption.

5.2.3 Printed Circuit Board (PCB) Identification Requirements

Each PCB used in the interface element hardware shall be clearly identifiable by an alphanumeric identification and, when applicable, a revision number. If track cuts, patch wires, or other circuit alterations are introduced to the PCB, then a new revision number shall be assigned.

5.2.4 Switches and Jumpers

If the interface element hardware contains switches and/or jumpers, they shall be fully documented for evaluation by the independent test laboratory.

5.2.5 Wired Communication Ports

Wired communication ports on the interface element hardware shall be clearly labeled.

5.2.6 Touch Screen Displays

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

5.2.7 Installation Requirements

The interface element hardware shall be installed in a secure area of the Gaming Equipment or in another secure location allowing only authorized access.

5.3 Interface Software Requirements

5.3.1 Software Identification

Interface element software shall contain sufficient information to identify the software and its version.

5.3.2 Software Validation

For software installed locally on the interface element, it shall be possible to authenticate that all critical components contained in the interface element software are valid each time the software is loaded for use, and where supported by the system, on demand as required by the regulatory body. Critical components may include, but are not limited to, elements that control the communications between the Gaming Equipment and the Gaming System or other components that are needed to ensure proper operation of the software. In the event of a failed authentication (i.e., program mismatch or authentication failure), the interface element software shall cease operation and display an appropriate error message. This error condition shall be communicated to the connected system when such a compatible system and protocol is supported.

NOTE: Program verification mechanisms will be evaluated on a case-by-case basis and may be certified by the independent test laboratory and approved by the regulatory body after taking industry best practices into consideration.

5.3.3 Independent Software Verification

It shall be possible to perform an independent integrity check of the interface element software from an outside source. This verification is required for all software that affects the integrity of regulated system operations. The verification shall be accomplished by being authenticated by a third-party

application run from the interface element and/or Gaming System, by allowing a third-party device to authenticate the media, or by allowing for removal of the media such that it can be verified externally. The independent test laboratory, prior to certification, shall evaluate the integrity check method.

5.3.4 Setup and Configuration Access

Access to the interface element software's setup and configuration menus shall be restricted to authorized access methods to ensure that only authorized personnel are allowed access.

5.3.5 Software Updates

If supported, a Gaming System may update interface element software if the following requirements are met:

a) Update functionality shall require an authorized access method to ensure that only authorized personnel are allowed access. The system can continue to locate and verify versions currently running but it cannot load code that is not currently running on the system without user intervention; and
b) A non-alterable audit log shall record the time/date of the software update and some provision shall be made to associate this log with which version(s) of code was downloaded, and the user who initiated the download.

NOTE: The above refers to loading of new system executable code only. Other program parameters may be updated as long as the process is securely controlled and subject to audit. The parameters will have to be reviewed on an individual basis.

5.4 Critical Non-Volatile (NV) Memory Requirements

5.4.1 General Statement

When the interface element's operation relies on locally stored critical NV memory, the requirements of this section shall apply.

NOTE: This section is not intended to preclude the use of alternate storage media types, such as hard disk drives, for the retention of critical data. Such alternate storage media is still expected to maintain critical data integrity in a manner consistent with the requirements in this section, as applicable to the specific storage technology implemented.

5.4.2 Critical NV Memory Backup

The interface element shall have a backup or archive capability, which allows the recovery of locally stored critical NV memory should a failure occur.

5.4.3 Clearing Critical NV Memory

An interface element shall not have a mechanism whereby an error or an unauthorized user can cause the loss of locally stored critical NV memory.

5.4.4 Critical NV Memory Errors

Critical NV memory storage shall be maintained by a methodology that enables errors to be identified. This methodology may involve signatures, checksums, redundant copies, database error checks, and/or other method(s) approved by the regulatory body.

5.4.5 Critical NV Memory Checks

Comprehensive checks of the locally stored critical NV memory shall be made during each power up and program resumption. Data that is not critical to interface element integrity is not required to be checked.

5.4.6 Unrecoverable Corruption of Critical NV Memory

An unrecoverable corruption of critical NV memory shall result in an error. Upon detection, the interface element software shall cease operations and display an appropriate error message. Additionally, the critical NV memory error shall cause any communication external to the interface element to cease.

5.5 Communications and Information Handling

5.5.1 Interface Communications

The communication between the interface element and the Gaming System shall be through a secure mechanism, using a secure communication protocol which ensures that the erroneous data or signals do not adversely affect the integrity or operation, and does not allow any external connection to directly access the internal components, software, or data of the Gaming Equipment. In addition, the interface element shall:

a) Be based on a specific defined protocol or a specific set of defined commands and as a result of these commands, retrieve information for an external request;
b) Place data in an area sufficiently segregated from the Gaming Equipment's software that is available to external requests or associated equipment; or
c) Be of a suitable design capable of supplying requested information while isolating the external request or equipment from the Gaming Equipment's internal components, software, or data.

5.5.2 Information Buffering

If unable to communicate the required "Significant Events and Metering Information" or applicable information pertaining to "Online Wagering Instrument Issuance" to the applicable Gaming System, the interface element shall provide a means to preserve the information until such time as it can be communicated to the system.

a) This information shall be capable of being reviewed on demand, at the interface element level via an authorized access method to ensure that only authorized personnel are allowed access;
b) Gaming operations may continue until the information is overwritten and lost at which point the Gaming Equipment shall disable. There shall be a method to check for corruption of the information storage locations; and
c) Once communication with the Gaming System is reestablished, the interface element shall accurately relay all buffered information to the system.

5.5.3 Information Protection

Any interface element that locally stores "Significant Events and Metering Information" or applicable information pertaining to "Online Wagering Instrument Issuance" shall not have means to compromise such information and shall not allow the removal of its information until that information has been successfully transferred and acknowledged by the applicable Gaming System.

Appendix A: Internal Controls for Gaming Venues

A.1 Introduction

A.1.1 General Statement

This appendix sets forth recommended procedures and practices for gaming operations which, if required by a regulatory body, will be reviewed in an operational audit as a part of the gaming environment evaluation, including, but not limited to handling various wagering instrument and financial transactions, wagering instrument management, review of the operational processes that are critical to compliance, storing and/or processing sensitive information, fundamental practices relevant to the limitation of risks, and any other objectives established by the regulatory body.

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

A.2 Internal Control Procedures

A.2.1 Internal Control Procedures

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

A.2.2 Information Management

The operator's internal controls shall include the processes for maintaining the recorded information specified within this standard for a period of five years or as otherwise specified by the regulatory body.

A.2.3 Risk Management

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

a) Automated and manual risk management procedures;
b) Personnel management, including access controls and segregation of duties;
c) Information regarding identifying and reporting fraud and suspicious conduct;
d) Controls ensuring regulatory compliance;
e) Description of Anti-Money Laundering (AML) compliance standards, including procedures for detecting structuring to avoid reporting requirements;
f) Description of all software applications that comprise the Gaming System;
g) Description of all integrated third-party service providers; and
h) Any other information required by the regulatory body.

A.3 General Operating Procedures

A.3.1 Player Protection Information

Player protection information shall be available to the player via external signage, forms, or brochures available at the gaming site. The player protection information shall contain at a minimum:

a) Information about potential risks associated with excessive gaming, and where to get help for a gambling problem;
b) A statement that no underage persons are permitted to participate in gaming;
c) A list of the available player protection measures that can be invoked by the player, such as self-imposed exclusion, and information on how to invoke those measures;
d) Contact information or other means for reporting a complaint/dispute; and
e) Contact information for the regulatory body and/or a link to their website.

A.3.2 Responsible Gaming

The operator shall have policies and procedures in place which facilitate interaction with players whenever their gaming behavior indicates a risk of the development of a gambling problem. Personnel interacting directly with players shall be trained to ensure they understand problem gambling issues and know how to respond to them.

A.4 Gaming Procedures and Controls

A.4.1 Evaluating Theoretical and Actual Return to Player Percentages

The operator shall maintain accurate and current documentation (e.g., PAR sheets) indicating the theoretical return to player (RTP) percentages for each house-banked game based on adequate levels of credits wagered, as well as the number of credits that may be played, the payout schedule and other information descriptive of the particular type of game. In addition:

a) Records shall be maintained for each game indicating the initial theoretical RTP percentage, dates and type of changes made affecting the game's theoretical RTP percentage, and the recalculation of theoretical RTP percentage because of the changes.
b) Each change to a game's theoretical RTP percentage, including adding and/or changing progressive jackpots, shall result in that game being treated as new for all reports and records.
c) If bonusing awards or promotional awards are included in the reports and records for the game, it shall be in a manner that prevents distorting the actual RTP percentages of the affected paytables.
d) The operator shall have procedures in place to, as required by the regulatory body, compare the theoretical and actual RTP percentage to identify, investigate, and resolve large variances between these two values.

A.4.2 Disabling Gaming

There shall be established procedures for disabling a game or Gaming Equipment. When a game or Gaming Equipment is disabled, an entry shall be made in an audit log that includes the date and time of disable and its reason.

A.4.3 Taxation

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

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

A.5 Monitoring Procedures

A.5.1 Anti-Money Laundering (AML) Monitoring

The operator is required to develop and implement AML procedures and policies that adequately address the risks posed by gaming for the potential of money laundering and terrorist financing. At a minimum, the AML procedures and policies shall provide for:

a) A system of internal controls to assure ongoing compliance with the local AML regulations and standards observed by the regulatory body;
b) Up to date training of personnel in the identification of unusual or suspicious transactions;
c) Assigning an individual or individuals to be responsible for all areas of AML by the operator including reporting unusual or suspicious transactions;
d) Monitoring applicable Gaming Equipment for cashable player funds added and cashed out without associated game play;
e) Ensuring that aggregate transactions over a defined period may require further due diligence checks and may be reportable to the relevant organization(s) if they exceed the threshold prescribed by the regulatory body;
f) Use of any automated data processing systems to aid in assuring compliance; and
g) Periodic independent tests for compliance with a scope and frequency as required by the regulatory body. Logs of all tests shall be maintained.

A.5.2 Monitoring for Collusion and Fraud

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

a) Identifying and/or refusing to accept suspicious wagers at a live game which may indicate cheating, manipulation, interference with the regular conduct of a game, or violations of the integrity of any game on which wagers were made.
b) Reasonably detecting irregular patterns or series of wagers to prevent player collusion in live games.

c) Reasonably detecting and preventing situations where players in games may be using unauthorized devices at a game or Gaming Equipment to create an unfair advantage during game play, such as:
   i. Projecting or predicting the outcome of a game;
   ii. For card games, tracking the cards played and cards remaining to be played;
   iii. Analyzing the probability of the occurrence of an event relating to a game; or
   iv. Analyzing the strategy for playing or wagering to be used in a game, unless allowed by the rules of the game.

A.6 Gaming Venue Specifications

A.6.1 General Statement

The Gaming Venue will be required to meet the applicable aspects of the appropriate policy and/or procedure documents as determined by the operator in consultation with the regulatory body. To maintain the integrity of gaming operations, Gaming Venues may be subject to an additional verification audit as required by the regulatory body.

A.6.2 Gaming Equipment

The Gaming Venue shall provide a secure location for the placement, operation, and usage of Gaming Equipment. Security policies and procedures shall be in place and reviewed as required by the regulatory body to ensure that risks are identified, mitigated, and underwritten by contingency plans. In addition:

a) Gaming Equipment shall be installed according to a defined plan and records of all installed Gaming Equipment shall be maintained.
b) Gaming Equipment shall be sited or protected to reduce the risks from:
   i. Environmental threats and hazards;
   ii. Opportunities for unauthorized access;
   iii. Power failures; and
   iv. Other disruptions caused by failures in supporting utilities.
c) To ensure its continued availability and integrity, Gaming Equipment shall be correctly maintained, inspected, and serviced at regular intervals to ensure that it is free from defects or mechanisms that could interfere with its operation.
d) Prior to disposal or re-use, Gaming Equipment containing storage media shall be checked to ensure that any licensed software and sensitive information has been removed or securely overwritten (i.e., not just deleted).

A.6.3 Gaming Procedures

The following procedures shall be in place for gaming operations within the Gaming Venue, which shall be reviewed as required by the regulatory body to ensure that risks are identified, mitigated, and underwritten by contingency plans:

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

b) Procedures to prevent any person from tampering with or interfering with the operation of any Gaming Equipment or game;
c) Procedures to describe the operations and the servicing of Gaming Equipment, including the handling of error conditions and performing reconciliations; and
d) Procedures to ensure accessibility requirements observed by the regulatory body are met for the installation of Gaming Equipment.

A.6.4 Live Game Procedures

In addition to the "Gaming Procedures" above, the following procedures shall be in place for live games:

a) Distinct procedures must be established for each live game, and any new games must have their procedures formulated and implemented prior to being made available to players. It is permissible to reference common procedures within these new procedures, provided that all game-specific requirements are adequately addressed.
b) The following procedures shall be in place for the live game personnel, including gaming attendants, as required by the regulatory body:
    i. Personnel shall undergo adequate training to provide live games in a fair way according to documented procedures and game rules. Evidence of training and periodic refresher training shall be maintained;
    ii. Personnel shall be trained in, and regularly reminded of, any physical behavior which is prohibited or mandated (including hand signals, talking, the handling of the cards, etc.);
    iii. Policies and procedures concerning rotations, shift patterns and allocation shall be documented, including how gaming attendants are allocated to tables/games (i.e., without prior knowledge of which tables/games they will be serving and with their time-on-game set at a level to deter harmful relationships being developed), and changes in gaming attendants during exceptional circumstances;
    iv. The retention of documentation shall be robust, allowing personnel records to be audited and investigations to be performed where personnel are either involved directly or where their presence in a particular place and/or time, is crucial to understanding a chain of events;
    v. A supervisor shall always be present when live games are taking place;
    vi. Staffing logs shall be maintained for each table/game; and
c) Procedures regarding anomalous events which may occur during live games shall be documented and understood by staff, including, but not limited to:
    i. Electronic wager station or live game management component malfunctions;
    ii. Dropped cards;
    iii. Misdeals;
    iv. Re-spins;
    v. Aborted games; and
    vi. Table/game closure.
d) Consistent card shuffling procedures, including a verification of the card count, frequency of shuffling, and cases for reshuffling, shall be in place. The shuffling of cards shall be logged.
e) A defined procedure shall exist for the accounting of the physical player chips.

f) Procedures shall be in place to demonstrate that a single member of personnel would not be able to undertake all duties concerning game management and that there is segregation of responsibilities prior to play, during play and after play.
g) Variations in the operation of card shufflers and shoes, roulette wheels, ball blowers, dice shakers or other equipment shall be incorporated into the game procedures to maintain randomness.
h) Procedures shall be in place to ensure card shoes and similar specialized devices and physical randomness devices are tamper-proof once they have been loaded to preclude interference prior to and during play.
i) Procedures shall be in place to maintain game logs and collate game events into statistics which can be analyzed for trends relating to game performance, personnel and/or locations in the Gaming Venue, including those for supervisors, shifts, procedure violations, as well as other incidents, irregularities, and errors.

A.6.5 Management of Consumables

Consumables used in the Gaming Venue shall meet minimum standards as determined by the regulatory body as well as the following requirements:

a) Procedures shall be implemented for tracking the inventory of consumables from receipt, through storage, installation, use, retirement, and destruction. All consumables shall have an associated audit trail which shows which designated staff had access to the consumables at any given time for any given operation;
b) Periodic random inspections shall be performed on the consumables in use, from disbursement to retirement; and
c) Used consumables shall be destroyed in a manner which prevents their accidental re-use in gaming operations, and which puts them permanently beyond use.

A.6.6 Surveillance and Recording

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

a) Covers the defined gaming areas with sufficient detail to confirm whether the live game rules and procedures were followed and identify any discrepancies;
b) Is captured in such a way that precludes interference or deletion;
c) Can be reviewed by the operator and/or regulatory body in the event of a player complaint/dispute; and
d) Is kept for at least ninety days or as required by the regulatory body.

Glossary of Key Terms

Access Control – The process of granting or denying specific requests for obtaining and using sensitive information and related services specific to a system; and to enter specific physical facilities which house critical network or system infrastructure.

Algorithm – A finite set of unambiguous instructions performed in a prescribed sequence to achieve a goal, especially a mathematical rule or procedure used to compute a desired result. Algorithms are the basis for most computer programming.

Attendant Paid Award – Any award from a single game or feature which is not capable of being paid by the Gaming Equipment itself.

Authentication – Verifying the identity of a user, process, software package, or device, often as a prerequisite to allowing access to resources in a system.

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

Barcode – An optical machine-readable representation of data, including barcodes found on wagering instruments and cards.

Barcode Reader – A device that is capable of reading or interpreting a barcode. This may extend to some smartphones or other electronic devices that can execute an application to read a barcode.

Cancelled Credits – Amounts paid by an attendant or by system-based command which results from a player initiated cash-out that exceeds the physical or configured capability of the Gaming Equipment to make the proper payout amount.

Cashable Player Funds – Player funds that are redeemable for cash, including cashable promotional credits.

Cashable Promotional Credits (aka "Unrestricted Promotional Credits") – Promotional credits that are redeemable for cash.

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

Coupon – A wagering instrument that is used primarily for promotional purposes and which can be redeemed for cashable or non-cashable promotional credits.

Coupon Promotion In/Out – The total value of all promotional coupons accepted or paid out by the Gaming Equipment.

Credit Slip – A generated form used to record the return of chips from a live game to the cage, or the transfer of IOUs, markers, or negotiable checks from a live game to a cage or bankroll, as applicable.

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

Critical Control Program – A software program that controls behaviors relative to any applicable technical standard and/or regulatory requirement.

Critical Non-Volatile (NV) Memory – Memory used to store all data that is considered vital to the continued operation of the interface element.

Electronic Accounting Meter (aka "Software Meter" / "Soft Meter") – An accounting meter that is implemented in Gaming Equipment software.

Electronic Game – A Gaming Device, Electronic Table Game, or other form of Gaming Equipment which uses electronic components to conduct gameplay.

Electronic Signature – An electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the generated slip.

Electronic Table Game – The combination of hardware and software components that function collectively to electronically simulate a live table game or a live card game. An electronic table game may be fully-automated or dealer-controlled (semi-automated).

Electronic Wager Station – A player interface unit that permits player transactions and/or wagering to be conducted at a live game.

ESD, *Electro-Static Discharge* – The release of static electricity when two objects come into contact. It is the sudden flow of electricity between two electrically charged objects caused by contact, an electrical short, or a dielectric breakdown.

Fill Slip – A generated form used to record a transaction where a supply of chips, coins, or tokens is transferred from a bankroll to a live game or Gaming Equipment, as applicable.

Game Theme (aka "Personality Program") – The concept, subject matter, and methodology of design in which a game is built around, including artwork, game graphics, one or more paytables, sound effects, and music.

Gaming Device – An electronic or electro-mechanical device that at a minimum will utilize an element of chance, skill, or strategy, or some combination of these elements in the determination of prizes, contain some form of activation to initiate the selection process, and makes use of a suitable methodology for delivery of the determined outcome.

Gaming Equipment – A gaming device, electronic table game, electronic wager station, live game management component, kiosk, or any other critical electronic gaming component and its interface element intended for use with a Gaming System.

Gaming System – A Monitoring and Control System or a Validation System, or other critical systems relative to any applicable technical standard and/or regulatory requirement within a Gaming Venue.

Gaming Venue – A physical location or site where gaming activities take place, such as casinos, racetracks, card rooms, bingo halls, gaming halls, or other similar facilities where Gaming Equipment is installed, such as public establishments used for video lottery and other forms of distributed gaming.

GEAR, *Gaming Equipment Asset Registry* (aka "Slot File") – A database containing information of all Gaming Equipment in operation.

Handpay – Any payments made by an attendant when the game is incapable of making the proper payment. Examples include, but are not limited to, attendant paid awards, canceled credits, short pays, special pays, or other payouts made by an attendant.

Hash Algorithm – A function that converts a data string into an alpha-numeric string output of fixed length.

Interface Element (aka "SMIB, *Slot Machine Interface Board")* – A circuit board that interfaces the Gaming Equipment with the Gaming System, supporting protocol conversion between the equipment and the system.

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

Jumper – A removable connector (plug, wire, etc.) that electrically joins together or short-circuits two separate physical connections.

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

Kiosk – A player interface unit that may be used to perform regulated operations when interfaced with a compatible host Gaming System.

Live Game – A game conducted by a gaming attendant (e.g., dealer, croupier, etc.). Live games include, but are not limited to, live drawings, live card games, live table games, live keno games, live bingo games, and live play of other games as allowed by the regulatory body.

Live Game Management Component – A workstation for gaming attendants (e.g., dealer, croupier, etc.) to manage live game activity, such as a live table game or a live card game.

Monitoring and Control System – The hardware, software, firmware, communications technology, other equipment, as well as operator procedures implemented in order to continuously monitor Gaming Equipment via a secure communication protocol. This system is primarily tasked to provide logging, searching, and reporting of significant events, collection of individual device financial and meter data, reconciliation of meter data against counts.

Multi-Factor Authentication – A type of authentication which uses two or more of the following to verify a user's identity: Information known only to the user (e.g., a password, pattern, or answers to challenge questions); An item possessed by a user (e.g., an electronic token, physical token, or an identification card); A user's biometric data (e.g., fingerprints, facial or voice recognition).

Non-Cashable Promotional Credits (aka "Restricted Promotional Credits") – Promotional credits that have no cash redemption value.

Operator – A person or entity that oversees a gaming environment, using both the technological capabilities of the Gaming System as well as their own internal control procedures.

PAR Sheet – A specification sheet for a game that provides the theoretical return to player, hit frequency, symbol combination, number of reels, number of credits that can be accepted, and reel strip listing as applicable.

Password – An authentication credential, using a string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Paytable (aka "Variation") – The mathematical behavior of a game based upon the data from the manufacturer's PAR sheet, inclusive of the return percentage, and reflective of all possible payouts/awards.

PCB, *Printed Circuit Board* – A hardware component of a computer or other electronic device, consisting of a flat piece of a non-conductive, rigid material to which Integrated Circuits (ICs) and other electronic components such as capacitors, resistors, etc. are mounted. Electrical connections are made between the ICs and components using a copper sheet that is laminated into the overall board assembly.

Peripheral – An internal or external device connected to Gaming Equipment that supports credit acceptance, credit issuance, player interaction, or other specialized function(s).

PII, *Personally identifiable information* – Sensitive information that could potentially be used to identify a particular player. Examples include a legal name, date of birth, place of birth, social security number (or equivalent government identification number), driver's license number, passport number, residential address, phone number, email address, debit instrument number, credit card number, bank account number, or other personal information if defined by the regulatory body.

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

Promotional Award – An award that is redeemable for cash or promotional credits based on predefined player activity criteria that is based on predefined player activity that are tied to a specific promotional account or other predefined criteria that do not require player or gaming activity prior to redemption and are generally single instance use.

Promotional Credits – Cashable promotional credits and non-cashable promotional credits.

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

Risk – The likelihood of a threat being successful in its attack against a network or system.

RTP, *Return to Player* – A ratio of the 'total amount won' to the 'total amount wagered' by a player. Such a return may be "theoretical" (based on mathematical calculations or simulations) or "actual" (based on the metering supported by an enabled game).

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

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

Time Stamp – A record of the current value of the Gaming System date and time which is added to a message at the time the message is created.

Touch Screen – A video display device that also acts as a player input device by using electrical touch point locations on the display screen.

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

Validation System – The hardware, software, firmware, communications technology, other equipment, as well as operator procedures implemented in order to securely maintain records of wagering instruments, validate payment of wagering instruments, record successful or failed payments of wagering instruments, and control the purging of expired wagering instruments.

Voucher (aka "Ticket") **–** A wagering instrument which can be redeemed for cash or used to subsequently redeem for credits.

Voucher In/Out (aka "Ticket In/Out") – The total value of all wagering vouchers accepted or paid out by the Gaming Equipment.

Wagering Instrument – A printed or virtual representative of value, other than a chip or token and includes coupons and vouchers. A virtual wagering instrument is an electronic token exchanged between a player's device and the Validation System which is used for credit insertion and redemption.

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

Workstation – An interface for authorized personnel to access the regulated functions of the Gaming System. Examples of workstations include, but are not limited to, Cashier Stations and Live Game Management Components.