BERMUDA GAMING COMMISSION (BCGC)

BGC-3 CASINO GAMING
ELECTRONIC MONITORING SYSTEM STANDARDS

VERSION: 1.1

RELEASE DATE: OCTOBER 22, 2021

Table of Contents

Chapter 1: Introduction to Electronic Monitoring Systems

1.1 Introduction

1.1.1 ***General Statement.***

Pursuant to section 199 of the Gaming Act 2014 ('the Act"), this equipment standard prescribes criteria to be met for electronic monitoring systems.

The criteria are not exhaustive. All statutory requirements contained in the Gaming Act 2014 ("the Act") and the Gaming (Casino) Regulations 2018 ("the Regulations") shall be observed. Approval shall be valid for a maximum term of 10 years and all applicable legislation and standards must be met on an ongoing basis.

These standards are of general application and seek to take account of the wide diversity of institutions which may be licensed under the Act. There may be need for revision of the standard from time to time. Material changes in the standards will be published generally by issuing a revised standard.

The integrity and accuracy of the operation of an Electronic Monitoring System is highly dependent upon operational procedures, configurations, and the production environment's network infrastructure, and as such will require the development of internal processes and procedures to ensure that the system is configured and operated with the necessary level of security and control. Internal Controls will be established which prescribe the requirements for any system or component software and hardware, and their associated accounts.

1.2 Purpose of Equipment Standards

1.2.1 ***General Statement.***

The purpose of this equipment standard is as follows:

a) To eliminate subjective criteria in analyzing and certifying Electronic Monitoring Systems;
b) To test the criteria that impact the credibility and integrity of Electronic Monitoring Systems from both the revenue collection and patron's perspective;
c) To create a standard that will ensure bets on events are fair, secure, and able to be audited and operated correctly;

d) To recognize that the evaluation of internal control systems (such as anti-money laundering/anti-terrorist financing, Financial and Business processes) employed by the casino operators of the Electronic Monitoring System should not be incorporated into the laboratory testing of the standard but instead be included within the operational audit performed for local jurisdictions;

e) To construct a standard that can be easily revised to allow for new technology; and

f) To construct a standard that does not specify any particular design, method, or algorithm. The intent is to allow a wide range of methods to be used to conform to the standards, while at the same time encourage new methods to be developed.

1.2.2 ***No Limitation of Technology.***

This document must not be read in such a way that limits the use of future technology. The Commission may review this standard and may make revisions as necessary to incorporate standards for new and related technology.

1.3 Interpretation of this Document

1.3.1 ***Software Suppliers and Casino Operators.***

The components of an Electronic Monitoring System, although they may be constructed in a modular fashion, are designed to work seamlessly together. In addition, Electronic Monitoring Systems may be developed to have configurable features; the final configuration of which depends on the options chosen by the casino operator. From a testing perspective, it might not be possible to test all of the configurable features of an Electronic Monitoring System submitted by a software supplier in the absence of the final configuration chosen by the casino operator; however, the configuration that will be utilized in the production environment shall be communicated to the testing laboratory to facilitate creating a functionally equivalent test environment. Because of the integrated nature of an Electronic Monitoring System, there are several requirements in this document which may apply to both casino operators and suppliers. In these cases, where testing is requested for a “white-label” version of the system, a specific configuration will be tested and reported.

1.4 Testing and Auditing

1.4.1 ***Laboratory Testing.***

The testing laboratory will test and certify the components of the Electronic Monitoring System in accordance with the chapters of this equipment standard within a controlled test environment, as applicable. Any of these requirements which necessitate additional operational procedures to meet the intent of the requirement shall be documented within the evaluation report and used to supplement the scope of the operational audit.

1.4.2 ***Operational Audit.***

In addition to the testing and certification of Electronic Monitoring System components, the Commission may elect to require a periodic operational audit be conducted, using the recommended scope outlined within the following appendices of this equipment standard:

a) Appendix A: Operational Audit for Technical Security Controls. This includes, but is not limited to, a review of the operational processes that are critical to compliance, penetration testing focused on the external and internal infrastructure as well as the applications transferring, storing and/or processing of personal identification information (PII) and/or other sensitive information, and any other objectives established by the Commission; and

b) Appendix B: Operational Audit for Service Providers. This includes the assessment of providers of particular services, which may be offered directly by the casino operator or involve the use of third-party service providers, including, but not limited to evaluation of information security services, cloud services, gaming area services, and any other services which may be offered directly by the casino operator or involve the use of third-party service providers.

Chapter 2: Platform/System Requirements

2.1 Introduction

2.1.1 ***General Statement.***

If the Electronic Monitoring 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 Electronic Monitoring 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 Electronic Monitoring 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 Programme Requirements

2.3.1 ***General Statement.***

In addition to the requirements contained within this section, the “Verification Procedures” section of this document shall also be met.

2.3.2 ***Control Programme Self-Verification.***

The Electronic Monitoring System shall be capable of verifying that all critical control programme components contained on the system are authentic copies of the approved components of the system on demand using a method approved by the Commission. The critical control programme 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 programme 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 programme component is determined to be invalid.

2.3.3 ***Control Programme Independent Verification.***

Each critical control programme component of the Electronic Monitoring 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 testing laboratory, prior to system approval, shall evaluate the integrity check method.

2.4 System Functionality

2.4.1 ***Front-End Processor and Data Collector Functionality.***

Electronic Monitoring Systems may possess a Front-End Processor that gathers and relays all data from the connected Data Collectors to the associated database(s). The Data Collectors, in turn, collect all data from connected gaming machines. If the Front-End Processor maintains buffered/logging information, then a means shall exist which prevents the loss of critical information contained herein.

2.4.2 ***Wagering Instrument Functionality.***

Electronic Monitoring Systems which support the issuance and redemption of wagering instruments (vouchers and/or coupons) shall meet the applicable requirements established within the “Wagering Instruments” section of the BGC-1 Casino Gaming Machine Standards and the “System Server Requirements” of the BGC-4 Casino Gaming Cashless Wagering System Standards and other applicable jurisdictional requirements observed by the Commission.

2.4.3 ***Patron Account Management.***

Electronic Monitoring Systems which support gaming using patron accounts shall meet the applicable "Patron Account Requirements" the "System Server Requirements" and the "Patron Account Controls" of the *BGC-4 Casino Gaming Cashless Wagering System* Standards and other applicable jurisdictional requirements observed by the Commission.

2.5 Hand Pay Slip Requirements

2.5.1 ***Hand Pay Slip Messages.***

An Electronic Monitoring System must have an application or facility that captures and processes every hand pay message from each gaming machine. Hand pay messages must be created for;

a) Attendant Paid Jackpot Payouts: Any award in which the amount is not capable of being paid by the gaming machine itself; and
b) Payout of Cancelled Credits: Any patron-initiated cash-out amount that exceeds the physical or configured capability of the gaming machine to make the proper payout amount.

2.5.2 ***Hand Pay Slip Information.***

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

a) Type of slip (e.g., jackpot payout, payout of cancelled credits, short pay, special pay, etc.);
b) Preprinted or concurrently-printed sequential number;
c) Date and Time (shift if required);
d) Gaming machine number;
e) Amount of payout (in local currency), or description of merchandise prize awarded;
f) For Attendant Paid Jackpot Payouts:
    i. Game outcome (e.g., reel symbols, multi-line payout, winning poker hand, etc.);

ii. Taxation indication, if applicable;

iii. Additional payout, if applicable.

iv. Total before taxes and taxes withheld, if applicable;

v. Amount to patron; and

vi. Total amount wagered;

g) Soft meter readings; and
h) Relevant signatures required by the Commission.

2.6 Information to be Maintained

2.6.1 ***Data Retention and Time Stamping.***

The Electronic Monitoring System shall be capable of maintaining and backing up all recorded data as discussed within this section in such manner as to be accessible upon request by the Commission for a period of not less than 7 years.

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).

2.6.2 ***Gaming Machine Information.***

Gaming machine information to be maintained and backed up by the Electronic Monitoring System shall include for each gaming machine, as applicable:

a) Unique interface element/location identification number for each gaming machine;
b) Gaming machine identification number or description (e.g. serial number, manufacturer);
c) Machine configuration data (e.g., button panel, top box, communications, progressives, etc.);
d) Game configuration data (e.g., paytable, denomination, etc.);
e) Theoretical return to player (RTP) of the gaming machine; and
f) Control programme(s) within gaming machine.

2.6.3 ***Significant Event Information.***

Significant event information to be maintained and backed up by the Electronic Monitoring System shall include, as applicable—

a) Failed account access attempts, including IP Address;
b) Programme error or authentication mismatch;
c) Significant periods of unavailability of any critical component of the system (any length of time gaming is halted for all patrons, and/or transactions cannot be successfully completed for any user);
d) System voids, overrides, and corrections;
e) Changes to live data files occurring outside of normal programme 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 personal identification information (PII) and other 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 Commission.

2.6.4 ***User Access Information.***

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

a) Employee name and title or position;
b) User identification;
c) Full list and description of functions that each group or user account may execute;
d) The date and time the account was created;
e) The date and time of last 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 (if applicable); and
i) The current status of the user account (e.g., active, inactive, closed, suspended, etc.).

2.7 Reporting Requirements

2.7.1 ***General Reporting Requirements.***

The Electronic Monitoring System shall be capable of generating the information needed to compile financial reconciliation and variance reports as may be required by the legislation or by written direction of the Commission. In addition to meeting the requirements in the section above for "Data Retention and Time Stamping", the following requirements shall apply for required reports—

a) The system shall be able to provide the reporting information on demand, on a daily basis, and for other intervals required by the Commission (e.g., month-to-date (MTD), year-to-date (YTD), life-to-date (LTD), etc.); and
b) Each required report shall contain:
    i. The casino 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.

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

2.7.2 ***Gaming Machine Performance Reports.***

The Electronic Monitoring System shall be able to provide the following information needed to compile one or more reports for Net Win/Revenue Report including, as applicable:

a) By machine or socket ID:
   i. Denomination or an indication that the machine is a multi-denomination machine;
   ii. Gaming machine number and game type;
   iii. Credits bet;
   iv. Metered or actual drop (system configurable);
   v. Actual hand pay slips issued;
   vi. Net Win/Revenue;
   vii. Theoretical RTP percentage;
   viii. Actual RTP percentage;
   ix. Percentage variance (theoretical RTP vs. actual RTP); and
b) By denomination and in total:
   i. Weighted average theoretical hold (i.e., floor par);
   ii. Combined actual RTP percentage (all win divided by all credits bet);
   iii. Percentage variance (floor par vs. combined actual RTP percentage); and
   iv. Projected dollar variance (i.e., total coin in times the percentage variance).

NOTE: Floor pars are the sum of the theoretical RTP percentages of all machines within a denomination weighted by coin in contribution.

2.7.3 ***Gaming Machine Comparison Reports.***

The Electronic Monitoring System shall be able to produce the following reports that compare metered amounts to actual amounts shall include a dollar variance and a percentage variance. The percentage variance is the dollar variance divided by the metered amount.

a) Metered vs. Actual Wins Comparison Reports. These reports are to include comparisons of metered wins vs. actual wins. “Metered win” equals “meter coin in” (-) “meter coin out” (-) “meter machine paid progressive payout” (-) “meter machine paid external bonus payout” (-) “total of meters accumulating attendant payouts” (excluding attendant paid cancelled credits);
b) Metered vs. Actual Hand Pay Comparison Reports. These reports are to include comparisons of metered amounts to actual amounts for each type of attendant hand pay;
c) Metered vs. Actual Drop Comparison Reports. These reports are to include comparisons of metered amounts to actual amounts for each medium dropped (e.g., bills, wagering instruments, etc.); and

d) Such other financial reconciliation and variance reports as may be required by the gaming law or by written direction of the Commission.

2.7.4 ***Significant Events and Alterations Reports.***

.

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

a) The date and time of the significant event or alteration;
b) Event/component identification;
c) Identification of user(s) who performed and/or authorised 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: Interface Element Requirements

3.1 Introduction

3.1.1 ***General Statement.***

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

3.2 Hardware Requirements

3.2.1 ***Printed Circuit Board (PCB) Identification Requirements.***

Each PCB used in an interface element 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.

3.2.2 ***Switches and Jumpers***

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

3.2.3 ***Wired Communication Ports.***

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

3.3 Software Requirements

3.3.1 ***Software Identification.***

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

3.3.2 ***Software Validation.***

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 machine and the Electronic Monitoring System or other components that are needed to ensure proper operation of the software.

NOTE: Programme verification mechanisms will be evaluated on a case-by-case basis and may be approved by the Commission and the testing laboratory after taking industry best practices into consideration.

3.3.3 ***Software Updates.***

If supported, an Electronic Monitoring System may update interface element software if the following requirements are met:

a) Update functionality must be, at a minimum, password-protected, and at an administrator level. 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 must record the time/date of the software update and some provision must 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.

3.3.4 ***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, 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 testing laboratory, prior to system approval, shall approve the integrity check method.

3.4 Security Requirements

3.4.1 ***Installation Requirements.***

The interface element shall be installed in secure area of the gaming machine or shall employ a secure communication method between the gaming machine and the interface element.

3.4.2 ***Configuration Access Requirements.***

The interface element setup/configuration menu(s) shall be not be available unless using an authorized access method.

3.5 Critical Data Requirements

3.5.1 ***General Statement.***

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

3.5.2 ***Backup Requirements.***

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

3.5.3 ***Comprehensive Checks.***

Comprehensive checks of the locally stored critical data 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.

3.5.4 ***Clearing Critical Data.***

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

3.6 Communication Requirements

3.6.1 ***Address Requirements.***

The interface element shall allow for the association of a unique identification number to be used in conjunction with an Electronic Monitoring System. This identification number will be used by the system to track all mandatory information of the associated gaming machine. Additionally, the system shall not allow for duplicate entries of this identification number.

3.6.2 ***System Communications.***

The communication between the interface element and the Electronic Monitoring System shall be through a secure mechanism, using a robust communication protocol that ensures that the wrong 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 machine. 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 machine'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 machine internal components, software or data.

3.6.3 ***Significant Events and Metering.***

The following information shall be generated on a gaming machine and communicated via the interface element to the Electronic Monitoring System for storage utilizing an approved communication protocol.

a) Significant event information listed within the "Significant Event Log" section of the *BCGC-1 Gaming Machine Standard* must be communicated and recorded as applicable. Each event must be stored in a database, which includes the following:
    i. The date and time which the event occurred;
    ii. Identity of the gaming machine 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 listed within the "Electronic Accounting and Occurrence Meters" section of the *BCGC-1 Gaming Machine Standard* must be communicated and recorded as applicable. Metering information on the Electronic Monitoring System must be:
    i. Stored in a database in credit units equal to the denomination, or in local currency; and
    ii. Labeled so they can be clearly understood in accordance to their function.

NOTE: This information may be either read directly from the gaming machine or relayed using a delta function. If the Electronic Monitoring System retrieves any of this information directly from the gaming machine, sufficient controls must be in place to ensure accuracy of the information.

3.6.4 ***Information Buffering.***

If unable to communicate the required information to the Electronic Monitoring System, the interface element shall provide a means to preserve all locally stored critical data until such time as it can be communicated to the system.

a) Gaming machine operation may continue until critical data will be overwritten and lost at which point the gaming machine shall disable. There shall be a method to check for corruption of the above data storage locations; and

b) Once communication with the system is reestablished, the interface element shall accurately relay all buffered critical data to the system.

Appendix A: Operational Audit for Technical Security Controls

A.1 Introduction

A.1.1 ***General Statement.***

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

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

NOTE: It is also recognized that additional technical security controls which are not specifically included within this standard will be relevant and required for an operational audit as determined by the casino operator and/or Commission within their rules, regulations, and internal controls.

A.2 System Operation & Security

A.2.1 ***System Procedures.***

The casino operator shall be responsible for documenting and following the relevant Electronic Monitoring System procedures and security standards, as required by the Commission, including procedures to:

a) Monitor the critical components and the transmission of data of the entire system, including communication, data packets, networks, as well as the components and data transmissions of any third-party services involved, with the objective of ensuring integrity, reliability and accessibility;
b) Maintain all aspects of security of the system to ensure secure and reliable communications, including protection from hacking or tampering;
c) Define, monitor, and document, as well as report, investigate, respond to, and resolve security incidents, including detected breaches and suspected or actual hacking or tampering with the system;
d) Monitor and adjust resource consumption and maintain a log of the system performance, including a function to compile performance reports; and
e) Investigate, document, and resolve malfunctions, which address the following:
    i. Determination of the cause of the malfunction;
    ii. Review of relevant records, reports, logs, and surveillance records;
    iii. Repair or replacement of the critical component;
    iv. Verification of the integrity of the critical component before restoring it to operation;
    v. Filing an incident report with the Commission and documenting the date, time and reason for the malfunction along with the date and time the system is restored; and
    vi. Voiding plays and pays if a full recovery is not possible.

A.2.2 ***Physical Location of Servers.***

The Electronic Monitoring System servers and databases shall be held in a restricted and secure area which shall be on the casino premises unless otherwise agreed in writing by the Commission. In addition, restricted and secure area shall—

a) Have sufficient protection against alteration, tampering or unauthorised access;
b) Be equipped with a surveillance system that shall meet the statutory requirements;
c) Be protected by security perimeters and appropriate entry controls to ensure that access is restricted to only authorised personnel;
    i. Physical access shall have a multi-factor authentication process unless the location is staffed at all times; and
    ii. Any attempts at physical access are recorded in a secure log; and

d) Be equipped with controls to provide physical protection against damage from fire, flood, and other forms of natural or manmade disaster (e.g., hurricane, earthquake, etc.).

A.2.3 ***Logical Access Control.***

The Electronic Monitoring System shall be logistically secured against unauthorised access by authentication credentials allowed by the Commission, such as passwords, multi-factor authentication, digital certificates, PINs, biometrics, and other access methods (e.g., magnetic swipe, proximity cards, embedded chip cards).

a) The Electronic Monitoring System shall restrict access by employees in accordance with job functions and responsibilities, shall prevent access by unauthorized parties, and shall detect possible unauthorized access and mitigate to the greatest extent possible the information accessible;
b) Each user account shall have their own individual authentication credential whose provision shall be controlled through a formal process, which shall include periodic review of access rights and privileges. The use of generic accounts shall be limited, and where used the reasons for their use shall be formally documented;
c) Authentication credential records for secret information shall be maintained either manually or by systems that automatically record authentication changes and force authentication credential changes;
d) Any authentication credentials stored on the system shall be either encrypted or hashed to the cryptographic algorithms that meet current industry accepted standards, such as ISO/IEC 19790, FIPS 140-2, or equivalent;
e) A fallback method for resetting authentication credentials (e.g., forgotten passwords) shall be at least as strong as the primary method. A multi-factor authentication process shall be employed for these purposes;
f) Lost or compromised authentication credentials and authentication credentials of terminated users shall be deactivated, secured or destroyed as soon as reasonably possible;
g) The system shall have multiple security access levels to control and restrict different classes of access to the server, including viewing, changing or deleting critical files and directories. Procedures shall be in place to assign, review, modify, and remove access rights and privileges to each user, including:
    i. Allowing the administration of user accounts to provide an adequate separation of duties;

ii. Limiting the users who have the requisite permissions to adjust critical system parameters; and
iii. The enforcement of adequate authentication credential parameters such as minimum length, and expiration intervals.

h) Procedures shall be in place to identify and flag suspect accounts to prevent their unauthorised use, which includes:
   i. Having system administrator notification and user lockout or audit trail entry, after a maximum number of three incorrect attempts at authentication;
   ii. Flagging of suspect accounts where authentication credentials may have been stolen; and
   iii. Invalidating accounts and transferring critical stored account information into a new account.

i) Any logical access attempts to the system applications or operating systems shall be recorded in a secure log**;**

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

k) Restrictions on connection times such as but not necessarily limited to session timeouts shall be used to provide additional security for high-risk applications, such as remote access.

NOTE: Where passwords are used as an authentication credential, it is recommended that they are at least eight characters in length.

A.2.4 ***User Authorisation.***

The Electronic Monitoring System shall implement the following user authorisation requirements:

a) A secure and controlled mechanism shall be employed that can verify that the critical component is being accessed by authorised personnel on demand and on a regular basis as required by the Commission;

b) When used, automated equipment identification methods to authenticate connections from specific locations and equipment shall be documented and shall be included in the review of access rights and privileges;

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

d) Where user sessions are tracked for authorisation, the user session authorisation information shall always be created randomly, in memory, and shall be removed after the user's session has ended.

A.2.5 ***Server Programming.***

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

A.2.6 ***Verification Procedures.***

There shall be procedures in place for verifying that the critical control programme components of the Electronic Monitoring System in the production environment are identical to those approved by the Commission.

a) Signatures of the critical control programme components shall be gathered from the production environment through a process to be approved by the Commission, and shall be performed:
   i. Upon installation/updates of components;
   ii. Upon power up or recovery from a shutdown state;
   iii. At least once every 24 hours; and
   iv. On demand.

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

c) The output of the process shall include the current and expected signature results and be stored in an unalterable format, which detail the verification results for each critical control programme authentication and:
   i. Be recorded in a system log or report which shall be retained for a period of ninety days or as otherwise specified by the Commission;
   ii. Be accessible by the Commission in a format which will permit analysis of the verification records by the Commission; and
   iii. Comprise part of the system records which shall be recovered in the event of a disaster or equipment or software failure.

d) Any failure of verification of any component of the system shall require a notification of the authentication failure being communicated to the casino operator and Commission as required; and
e) There shall be a process in place for responding to authentication failures, including determining the cause of the failure and performing the associated corrections or reinstallations needed in a timely manner.

A.2.7 ***Electronic Document Retention System.***

Reports listed under the "Reporting Requirements" within this standard and required by the Commission may be stored in an electronic document retention system provided that the system—

a) Is properly configured to maintain the original version along with all subsequent versions reflecting all changes to the report for reports that are stored in an alterable format;
b) Maintains a unique signature for each version of the report, including the original;
c) Retains and reports a complete log of changes to all reports including who (user identification) performed the changes and when (date and time);
d) Provides a method of complete indexing for easily locating and identifying the report including at least the following (which may be input by the user):
    i. Date and time report was generated;
    ii. Application or system generating the report;
    iii. Title and description of the report;
    iv. User identification of who is generating the report;
    v. Any other information that may be useful in identifying the report and its purpose;
e) Is configured to limit access to modify or add reports to the system through logical security of specific user accounts;
f) Is configured to provide a complete audit trail of all administrative user account activity;
g) Is properly secured through use of logical security measures (user accounts with appropriate access, proper levels of event logging, and document the version control, etc.);
h) Is physically secured with all other critical components of the Electronic Monitoring System; and
i) Is equipped to prevent disruption of report availability and loss of data through hardware and software redundancy best practices, and backup processes.

A.2.8 ***Asset Management.***

All physical or logical assets housing, processing or communicating sensitive information, including those comprising the operating environment of the Electronic Monitoring System and/or its components, shall be accounted for.

a) Procedures shall exist for adding new assets and removing assets from service;
b) Assets shall be disposed of securely and safely using documented procedures;
c) A policy shall be included on the acceptable use of assets associated with the system and its operating environment;
d) The designated "owner" of each asset is responsible for:
    i. Ensuring that information and assets are appropriately classified in terms of their confidentiality, integrity, accountability, and availability; and
    ii. Defining and periodically reviewing access restrictions and classifications.
e) A procedure shall exist to ensure that recorded accountability for assets is compared with actual assets at least annually or at intervals required by the Commission and appropriate action is taken with respect to discrepancies;
f) Copy protection to prevent unauthorised duplication or modification of licensed software may be implemented provided that:
    i. The method of copy protection is fully documented and provided to the testing laboratory, to verify that the protection works as described; or
    ii. The programme or component involved in enforcing the copy protection can be individually verified by the methodology approved by the Commission.
g) Prior to disposal or re-use, assets containing storage media shall be checked to ensure that any licensed software, as well as PII and other sensitive information has been removed or securely overwritten (i.e., not just deleted).

A.2.9 ***Critical Asset Register (CAR).***

A Critical Asset Register (CAR) shall be maintained for any assets that affect the functionality of the Electronic Monitoring System or has an influence on how PII and other sensitive information is stored/handled by the system. The structure of the CAR shall include hardware and software components and the inter-relationships and dependencies of the components. The following minimum items shall be documented for each asset:

a) The name/definition of each asset;
b) A unique ID that is assigned to each individual asset;

c) A version number of the asset listed;
d) Identifying asset characteristics (e.g., system component, database, virtual machine, hardware);
e) The "owner" responsible for the asset;
f) The geographical location of hardware assets; and
g) Relevance codes on the asset's role in achieving or ensuring the following classification criteria:
    i. Confidentiality of PII and other sensitive information (e.g., identification and transaction information);
    ii. Integrity of the system, specifically any asset that affects the functionality of the system and/or has an influence on how PII and other sensitive information is stored and/or handled;
    iii. Availability of PII and other sensitive information; and
    iv. Accountability of user activity, and how much influence the asset has on the user activity.

NOTE: For each of the above classification criteria a relevance code of 1, meaning no relevance (the asset can have no negative impact on the criteria), 2, meaning some relevance (the asset can have an impact on the criteria); or 3, meaning substantial relevance (the criteria are related to or dependent on the asset) shall be assigned.

A.3 Data Integrity

A.3.1 ***Data Security***

The casino operator shall provide a layered approach to security within the production environment to ensure secure storage and processing of data. The Electronic Monitoring System shall provide a logical means for securing PII and other sensitive information, including accounting, reporting, significant event, or other patron and gaming data, against alteration, tampering, or unauthorised access.

a) Appropriate data handling methods shall be implemented, including validation of input and rejection of corrupt data;
b) The number of workstations where critical applications or associated databases may be accessed shall be limited;
c) Encryption or password protection or equivalent security shall be used for files and directories containing data. If encryption is not used, the casino operator shall restrict users from viewing the contents of such files and directories, which at a minimum shall provide for the segregation of system duties and responsibilities as

well as the monitoring and recording of access by any person to such files and directories;

d) The normal operation of any equipment that holds data shall not have any options or mechanisms that may compromise the data;

e) No equipment may have a mechanism whereby an error will cause the data to automatically clear;

f) Any equipment that holds data in its memory shall not allow removal of the information unless it has first transferred that information to the database or other secured component(s) of the system;

g) PII and other sensitive information shall be stored in areas of the server that are encrypted and secured from unauthorised access, both external and internal;

h) Production databases containing data shall reside on networks separated from the servers hosting any user interfaces;

i) Data shall be maintained at all times regardless of whether the server is being supplied with power; and

j) Data shall be stored in such a way as to prevent the loss of the data when replacing parts or modules during normal maintenance.

A.3.2 ***Data Alteration.***

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

a) Unique ID number for the alteration;

b) Data element altered;

c) Data element value prior to alteration;

d) Data element value after alteration;

e) Time and date of alteration; and

f) Personnel that performed alteration (user identification).

A.3.3 ***Backup Frequency.***

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

A.3.4 ***Storage Medium Backup.***

Audit logs, system databases, and any other PII or pertinent gaming data shall be stored using reasonable protection methods. The Electronic Monitoring System shall be designed to protect the integrity of this data in the event of a failure. Redundant copies of this data shall be kept on the system with open support for backups and restoration, so that no single failure of any portion of the system would cause the loss or corruption of data.

a) The backup shall be contained on a non-volatile physical medium, or an equivalent architectural implementation, so that should the primary storage medium fail, the functions of the system and the process of auditing those functions can continue with no critical data loss. If hard disk drives are used as backup media, data integrity shall be assured in the event of a disk failure;
b) Upon completion of the backup process, the backup media is immediately transferred to a location physically separate from the location housing the servers and data being backed up (for temporary and permanent storage):
    i. The storage location shall be secured to prevent unauthorised access and provides adequate protection to prevent the permanent loss of any data.
    ii. Backup data files and data recovery components shall be managed with at least the same level of security and access controls as the system.
c) Where the Commission allows for the use of cloud platforms, if the backup is stored in a cloud platform, another copy may be stored in a different cloud platform or region.

A.3.5 ***System Failure***

The Electronic Monitoring System shall have sufficient redundancy and modularity so that if any single component or part of a component fails, the functions of the system and the process of auditing those functions can continue with no critical data loss. When two or more components are linked a procedure shall be in place for the Electronic Monitoring System and components to be tested after installation but prior to use in a production environment to verify that:

a) The process of all gaming operations between the components shall not be adversely affected by restart or recovery of either component (e.g., transactions

are not to be lost or duplicated because of recovery of one component or the other); and

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

A.3.6 ***Accounting of Master Resets.***

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

A.3.7 ***Recovery Requirements.***

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

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

A.3.8 ***Uninterruptible Power Supply (UPS) Support.***

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

A.3.9 ***Business Continuity and Disaster Recovery Plan.***

A business continuity and disaster recovery plan shall be in place to recover gaming operations if the Electronic Monitoring System's production environment is rendered inoperable. Such plan shall consider disasters including, but not limited to, those caused by weather, water, flood, fire, environmental spills and accidents, malicious destruction, acts of terrorism or war, and contingencies such as strikes, epidemics, pandemics, etc. The business continuity and disaster recovery plan shall:

a) Address the method of storing PII and other sensitive information, including gaming data, to minimize loss. If asynchronous replication is used, the method for recovering information shall be described or the potential loss of information shall be documented;
b) Delineate the circumstances under which it will be invoked;
c) Address the establishment of a recovery site physically separated from the production site. Utilization of cloud platforms for this purpose will be evaluated on a case-by-case basis;
d) Contain recovery guides detailing the technical steps required to re-establish gaming functionality at the recovery site; and
e) Address the processes required to resume administrative operations of gaming activities after the activation of the recovered system for a range of scenarios appropriate for the operational context of the system.

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

A.4 Communications

A.4.1 ***General Statement.***

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

A.4.2 ***Connectivity.***

Only authorised devices shall be permitted to establish communications between any critical components of the system. The Electronic Monitoring System shall provide a method to:

a) Enroll and un-enroll critical components;
b) Enable and disable specific critical components;
c) Ensure that only enrolled and enabled critical components can participate in gaming operations; and
d) Ensure that the default condition for critical components shall be un-enrolled and disabled.

A.4.3 ***Communication Protocol.***

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

a) All protocols shall use communication techniques that have proper error detection and recovery mechanisms, which are designed to prevent intrusion, interference, eavesdropping and tampering. Any alternative implementations will be reviewed on a case-by-case basis and approved by the Commission;
b) All data communications critical to gaming or patron account management shall employ encryption and authentication;
c) Communications on the secure network shall only be possible between approved critical components that have been enrolled and authenticated as valid on the network. No unauthorised communications to components and/or access points shall be allowed;
d) Communications shall be hardened in order to be immune to all possible malformed message attacks; and

e) After a system interruption or shutdown, communication with all components necessary for system operation shall not be established and authenticated until the programme resumption routine, including any self-tests, are completed successfully.

A.4.4 ***Communications Over Internet/Public Networks***

Communications between any system components which takes place over internet/public networks, shall be secure by encrypting the data packets or by utilizing a secure communications protocol to ensure the integrity and confidentiality of the transmission. PII, sensitive information, bets, results, financial information, and patron transaction information shall always be encrypted over the internet/public network and protected from incomplete transmissions, misrouting, unauthorised message modification, disclosure, duplication or replay.

A.4.5 ***Wireless Local Area Network (WLAN) Communications***

Wireless Local Area Network (WLAN) communications, as allowed by the Commission, shall adhere to the applicable requirements specified for wireless devices and network security and is subject to approval by the Commission. Wireless communication between the Remote Patron Device and the Electronic Monitoring System must be encrypted in transit using a method (for example, AES, IPsec, WPA2 or WPA3) approved by the Commission.

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

A.4.6 ***Network Security Management***

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

a) All network management functions shall authenticate all users on the network and encrypt all network management communications;
b) The failure of any single item shall not result in a denial of service;
c) An Intrusion Detection System/Intrusion Prevention System (IDS/IPS) shall be installed which includes one or more components that can listen to both internal and external communications as well as detect or prevent:
    i. Distributed Denial of Service (DDOS) attacks;
    ii. Shellcode from traversing the network;
    iii. Address Resolution Protocol (ARP) spoofing; and
    iv. Other "Man-In-The-Middle" attack indicators and sever communications immediately if detected.
d) In addition to the requirements in (c), an IDS/IPS installed on a WLAN shall be able to:
    i. Scan the network for any unauthorised or rogue access points or devices connected to any access point on the network at least quarterly or if defined by the Commission;
    ii. Automatically disable any unauthorised or rogue devices connected to the system; and
    iii. Maintain a history log of all wireless access for at least the previous ninety days or as otherwise specified by the Commission. This log shall contain complete and comprehensive information about all wireless devices involved and shall be able to be reconciled with all other networking devices within the site or casino.
e) Network Communication Equipment (NCE) shall meet the following requirements:
    i. NCE shall be constructed in such a way as to be resistant to physical damage to the hardware or corruption of the contained firmware/software by normal usage;
    ii. NCE shall be physically secured from unauthorised access;
    iii. System communications via NCE shall be logically secured from unauthorised access; and
    iv. NCE with limited onboard storage shall, if the audit log becomes full, disable all communication or offload logs to a dedicated log server.
f) All entry and exit points to the network shall be identified, managed, controlled, and monitored on a 24/7 basis. In addition:
    i. All network hubs, services and connection ports shall be secured to prevent unauthorised access to the network; and
    ii. Unused services and non-essential ports shall be either physically blocked or software disabled whenever possible.
g) In cloud and virtualized environments, redundant server instances shall not run

under the same hypervisor. In addition:

i. Each server instance may perform only one function; and

ii. Alternative equivalently secure mechanisms will be considered as technology advances.

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

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

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

k) The casino operator shall monitor the system and network in order to prevent, detect, mitigate, and respond to cyberattacks.

A.4.7 ***Active and Passive Attacks.***

Appropriate measures shall be in place to detect, prevent, mitigate, and respond to common active and passive technical attacks. The casino operator shall have an established procedure to gather cyber threat intelligence and act on it appropriately.

A.4.8 ***Mobile Computing and Communications.***

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. Telecommuting shall not be permitted except under circumstances where the security of the endpoint can be guaranteed.

A.5 Third-Party Service Providers

A.5.1 ***Third-Party Communications.***

Where communications with third-party service providers are implemented, such as for patron loyalty programs, payment services (financial institutions, payment processors,

etc.), location services, information security services, cloud services, statistics/line services, and identity verification services, the following requirements apply:

a) The Electronic Monitoring System shall be capable of securely communicating with third-party service providers using encryption and strong authentication;
b) All login events involving third-party service providers shall be recorded to an audit file;
c) Communication with third-party service providers shall not interfere or degrade normal Electronic Monitoring System functions:
    i. Third-party service provider data shall not affect patron communications.
    ii. Third-party service providers shall be on a segmented network separate from network segments hosting patron connections;
    iii. Gaming shall be disabled on all network connections except for those within the production environment;
    iv. The system shall not route data packets from third-party service providers directly to the production environment and vice-versa; and
    v. The system shall not act as IP routers between the production environment and third-party service providers.
d) When an incident or error occurs that results in a loss of communication between the production environment and third-party service providers, the operator shall record the incident or error in a log along with the date and time of occurrence, its duration, nature, and a description of its impact on the system's performance.

A.5.2 ***Third-Party Services.***

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

a) Agreements with third-party service providers involving accessing, processing, communicating or managing the system and/or its components, or adding products or services to the system and/or its components shall cover all relevant security requirements;
b) The services, reports and records provided by the third-party service providers shall be monitored and reviewed annually or as required by the Commission;
c) Changes to the provision of third-party service providers, including maintaining and

improving existing security policies, procedures and controls, shall be managed, taking account of the criticality of systems and processes involved and re-assessment of risks;

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

e) When an incident or error occurs that results in a loss of communication with a third-party service provider, the casino operator shall record the incident or error in a log along with the date and time of occurrence, its duration, nature, and a description of its impact on the system's performance. This information shall be maintained for a period of ninety days, or as otherwise specified by the Commission;

A.5.3 ***Third-Party Data Processing.***

Unauthorised third-party service providers shall be prevented from viewing or altering PII and other sensitive information. Where PII and other sensitive information is shared with third-party service providers, formal data processing agreements shall be in place that states the rights and obligations of each party concerning the protection of the PII and other sensitive information. Each data processing agreement shall set out:

a) The subject matter and duration of the processing;
b) The nature and purpose of the processing;
c) The type of data to be processed;
d) How the data is stored;
e) The detail of the security surrounding the data;
f) The means used to transfer the data from one organization to another;
g) The means used to retrieve data about certain individuals;
h) The method for ensuring a retention schedule is adhered to;
i) The means used to delete or dispose of the data; and
j) The categories of data.

A.6 Technical Controls

A.6.1 ***Domain Name Service (DNS) Requirements.***

The following requirements apply to the servers used to resolve public or external Domain Name Service (DNS) queries used in association with the Electronic Monitoring System.

a) The casino operator shall utilize a secure primary DNS server and a secure secondary DNS server which are logically and physically separate from one another;
b) The primary DNS server shall be physically located in a secure data center or a virtualized host in an appropriately secured hypervisor or equivalent;
c) Logical and physical access to the DNS server(s) shall be restricted to authorised personnel;
d) Zone transfers to arbitrary hosts shall be disallowed;
e) A method to prevent cache poisoning, such as DNS Security Extensions (DNSSEC), is required;
f) Multi-factor authentication shall be in place; and
g) Registry lock shall be in place, so any request to change DNS server(s) will need to be verified manually.

A.6.2 ***Cryptographic Controls.***

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

a) PII and other sensitive information shall be encrypted if it traverses a network with a lower level of trust. Encryption shall also be applied for such PII and other sensitive information stored on portable computer systems (e.g., laptops, USB devices, etc.);
b) Data that is not required to be hidden but shall be authenticated shall use some form of message authentication technique;
c) Authentication shall use a security certificate from an approved organization, containing information about whom it belongs to, who it was issued by, valid dates, a unique serial number or other unique identification that can be used to verify the contents of the certificate;
d) The grade of encryption used shall be appropriate to the sensitivity of the data.
e) The use of encryption algorithms shall be reviewed periodically to verify that the current encryption algorithms are secure;
f) The encryption method shall include the use of different encryption keys so that encryption algorithms can be changed or replaced to correct weaknesses as soon as practical. Other methodologies shall be reviewed on a case-by-case basis; and

g) Encryption keys shall be stored on a secure and redundant storage medium after being encrypted themselves through a different encryption method and/or by using a different encryption key.

A.6.3 ***Encryption Key Management.***

The management of encryption keys shall follow defined processes established by the casino operator and approved by the Commission, which shall cover the following—

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

A.6.4 ***Critical Component Hardening***.

Configuration procedures for critical components shall address all known security vulnerabilities and be consistent with industry-accepted best practices for system hardening. The appropriateness and effectiveness of steps taken to harden critical components shall be regularly assessed and, if appropriate, changes shall be made to improve the hardening. These configuration procedures shall include the following:

a) All default or standard configuration parameters shall be removed from all components where a security risk is presented;
b) Only one primary function shall be implemented per server to prevent functions that require different security levels from co-existing on the same server;
c) Additional security features shall be implemented for any required services, protocols or daemons that are considered to be insecure;
d) System security parameters shall be configured to prevent misuse; and
e) All unnecessary functionality shall be removed, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

A.6.5 Generation and Storage of Logs

There shall be procedures in place to centrally monitor and manage user activities, exceptions, and information security events. Logs recording these items shall be:

a) Generated on each critical component of the system in order to monitor and rectify anomalies, flaws and alerts;
b) Stored for an appropriate period to assist in future investigations and access control monitoring;
c) Protected against tampering and unauthorised access; and
d) Reviewed periodically using a documented process. A record of each review shall be maintained.

A.7 Remote Access and Firewalls

A.7.1 ***Remote Access Security.***

Remote access is defined as any access from outside the system or system network including any access from other networks within the same site or casino. Pursuant to regulation 170, remote access shall only be allowed if authorised by the Commission and shall:

a) Be performed via a secured method, such as a multi-factor authentication process;
b) Establish the connection in a way that prevents unauthorised access to the system or the data transmitted between the user and the Electronic Monitoring System;
c) Have the option to be disabled;
d) Use a firewall or equivalent protection in conjunction with the connection;
e) Accept only the remote connections permissible by the firewall application and system settings;
f) Be limited to only the application functions necessary for users to perform their job duties:
    i. No unauthorised remote user administration functionality (adding users, changing permissions, etc.) is permitted; and
    ii. Unauthorised access to the operating system or to any database other than information retrieval using existing functions is prohibited.

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

A.7.2 ***Remote Access Procedures by Suppliers.***

A procedure for strictly controlled remote access shall be established. An Electronic Monitoring System may permit remote access by an authorised staff member of an approved gaming supplier (a "remote user") to the system and its associated components for product and user support or updates/upgrades, as permitted by the Commission and the casino operator pursuant to regulation 170. This remote access shall use user accounts reserved for this purpose which are:

a) Continuously monitored by the casino operator;
b) Disabled when not in use; and
c) Restricted through logical security controls to access only the necessary application(s) and/or database(s) for the product and user support or providing updates/upgrades.

A.7.3 ***Remote Access Activity Log.***

The remote access application shall maintain an activity log which updates automatically depicting all remote access information and transactions by a remote user pursuant to regulation 170(d), to include:

a) Date and time of access (when the connection was made and duration of connection);
b) The identity of the user(s) who performed and/or authorised the remote access;
c) Remote IP Addresses, Port Numbers, Protocols, and where possible, MAC Addresses;
d) The reason for access; and
e) Activity while logged in, including the specific areas accessed and details of any modifications or transactions.

NOTE: This activity log shall be regularly reviewed as required by the casino operator and/or the Commission.

A.7.4 ***Firewalls.***

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

a) The firewall shall be located at the boundary of any two dissimilar security domains;
b) A device in the same broadcast domain as the system host shall not have a facility that allows an alternate network path to be established that bypasses the firewall;
c) Any alternate network path existing for redundancy purposes shall also pass through at least one application-level firewall;
d) Only firewall-related applications may reside on the firewall;
e) Only a limited number of user accounts may be present on the firewall (e.g., network or system administrators only);
f) The firewall shall reject all connections except those that have been specifically approved;
g) The firewall shall reject all connections from destinations which cannot reside on the network from which the message originated (e.g., RFC1918 addresses on the public side of an internet firewall); and
h) The firewall shall only allow remote access using encryption that meets current industry accepted standards**,** such as ISO/IEC 19790, FIPS 140-2, or equivalent**.**

A.7.5 ***Firewall Audit Logs.***

Firewalls used to protect the production environment shall be able to log audit information in a manner to preserve and secure the information from loss or alteration. This information includes the following:

a) All changes to configuration of the firewall;
b) All successful and unsuccessful connection attempts through the firewall; and

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

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

A.8 Change Management

A.8.1 ***General Statement.***

A change management policy (CMP) is approved by the Commission for handling updates to the Electronic Monitoring System and its components based on the propensity for frequent system upgrades and chosen risk tolerance. For systems that require frequent updates, a risk-based change management programme may be utilized to afford greater efficiency in deploying updates. Risk-based CMPs typically include a categorization of proposed changes based on regulatory impact and define associated certification procedures for each category. The testing laboratory will evaluate the system and future modifications in accordance with the CMP approved by the Commission.

A.8.2 ***Programme Change Control Procedures.***

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

a) An appropriate software version control or mechanism for all software components, source code, and binary controls;
b) Records kept of all new installations and/or modifications to the system, including:
    i. The date of the installation or modification;
    ii. Details of the reason or nature of the installation or change such as new software, server repair, significant configuration modifications;
    iii. The component(s) to be changed including the unique identification number from the CAR, version information, and if the component being changed is

hardware, the physical location of this component;

iv. The identity of the user(s) performing the installation or modification; and

v. The identity of the user(s) responsible for authorising the installation or modification.

c) A strategy to cover the potential for an unsuccessful install or a field issue with one or more changes implemented under the CMP:

i. Where an outside party such as an App store is a stakeholder in the release process, this strategy shall cover managing releases through the outside party. This strategy may take into account the severity of the issue; and

ii. Otherwise, this strategy shall cover reverting back to the last implementation (rollback plan), including complete backups of previous versions of software and a test of the rollback plan prior to implementation to the production environment.

d) A policy addressing emergency change procedures;

e) Procedures for testing and migration of changes, including the identification of authorised personnel for signoff prior to release;

f) Segregation of duties within the release process; and

g) Procedures to ensure that technical and user documentation is updated as a result of a change.

A.8.3 ***System Development Life Cycle.***

The acquisition and development of new software shall follow defined processes established by the casino operator and approved by the Commission.

a) The production environment shall be logically and physically separated from the development and test environments. When cloud platforms are used, no direct connection may exist between the production environment and any other environment.

b) The delegation of responsibilities between the casino operator and/or supplier shall be established where applicable.

c) There shall be a documented method to develop software securely:

i. Following industry standards and/or best practices for coding; and

ii. Incorporating information security throughout the life cycle.

d) The documented test methodology shall include provisions to:

i. Verify that test software is not deployed to the production environment; and

ii. Prevent the use in testing of actual PII and other sensitive information, or

other raw production data.

e) All documentation relating to software and application development shall be available and retained for the duration of its life cycle.

A.8.4 ***Patches.***

The casino operator shall have patching policies approved by the Commission, whether developed and supported by the casino operator or by a third-party service provider. All patches should be tested whenever possible on a development and test environment configured identically to the target production environment. Under circumstances where patch testing cannot be thoroughly conducted in time to meet the timelines for the severity level of the alert and if authorised by the Commission, then patch testing should be risk managed, either by isolating or removing the untested component from the network or applying the patch and testing after the fact.

A.9 Technical Security Testing

A.9.1 ***Periodic Security Testing.***

On an annual basis, technical security tests on the production environment shall be performed to guarantee that no vulnerabilities putting at risk the security and operation of the Electronic Monitoring System exist.

a) These tests shall consist of a method of evaluation of security by means of an attack simulation by a third-party following a known methodology, and the analysis of vulnerabilities will consist in the identification and passive quantification of the potential risks of the system.

b) Unauthorised access attempts shall be carried out up to the highest level of access possible and shall be completed with and without available authentication credentials (white box/black box type testing). These allow assessments to be made regarding operating systems and hardware configurations, including but not limited to:

   i. UDP/TCP port scanning;

   ii. Stack fingerprinting and TCP sequence prediction to identify operating systems and services;

iii. Public Service Banner grabbing;
iv. Web scanning using HTTP and HTTPS vulnerability scanners; and
v. Scanning routers using BGP (Border Gateway Protocol), BGMP (Border Gateway Multicast Protocol) and SNMP (Simple Network Management Protocol).

c) Once completed, a report on the assessments shall be provided to the Commission, which shall include:
i. Scope of review;
ii. Name and company affiliation of the individual(s) who conducted the assessment;
iii. Date of the assessment;
iv. Findings;
v. Recommended corrective action, if applicable; and
vi. The casino operator's response to the findings and recommended corrective action.

A.9.2 ***Vulnerability Assessment.***

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

a) External Vulnerability Assessment – The targets are the network devices and servers which are accessible by a third-party (both a person and a company), by means of a public IP (publicly exposed), related to the system from which is possible to access PII and other sensitive information; and
b) Internal Vulnerability Assessment – The targets are the internal facing servers (within the DMZ, or within the LAN if there is no DMZ) related to the system from which is possible to access PII and other sensitive information. Testing of each security domain on the internal network shall be undertaken separately.

A.9.3 ***Penetration Testing.***

The purpose of the penetration testing is to exploit any weaknesses uncovered during the

vulnerability assessment on any publicly exposed applications or systems hosting applications processing, transmitting and/or storing PII and other sensitive information. The penetration testing shall include at least the following activities:

a) Network Layer Penetration Test – The test mimics the actions of an actual attacker exploiting weaknesses in the network security examining systems for any weakness that could be used by an external attacker to disrupt the confidentiality, availability and/or integrity of the network; and
b) Application Layer Penetration Test – The test uses tools to identify weaknesses in the applications with both authenticated and unauthenticated scans, analysis of the results to remove false positives, and manual testing to confirm the results from the tools and to identify the impact of the weaknesses.

A.9.4 ***Firewall Rules Review.***

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

Appendix B: Operational Audit for Service Providers

B.1 Introduction

B.1.1 *General Statement.*

This appendix sets forth procedures and practices for the assessment of providers of particular services, which will be reviewed in an operational audit as a part of the Electronic Monitoring System evaluation, including, but not limited to evaluation of information security services, cloud services, payment services (financial institutions, payment processors, etc.), location services, and any other services which may be offered directly by the casino operator or involve the use of third-party service providers.

B.2 Information Security Services

B.2.1 *Information Security Management System (ISMS) Audit.*

The casino operator or a third-party information security service provider used to provide management, support, security, or disaster recovery services for the system shall undergo a specific audit. Their Information Security Management System (ISMS) will be reviewed against common information security principles in relation to confidentiality, integrity and availability, as covered within the appendix for “Operational Audit for Technical Security Controls”, and this section. It may be acceptable to leverage the results of prior audits conducted by appropriately accredited vendors and qualified individuals, within the current audit period (e.g., within the past year), against standards such as ISO/IEC 27001, the NIST Cybersecurity Framework (CSF), or equivalent. Such leveraging will be noted in the audit report.

B.2.2 *Information Security Policy.*

An information security policy shall be in effect to describe the ISMS’s approach to managing information security and its implementation. The information security policy shall:

a) Have a provision requiring review at planned intervals and when changes occur to the Electronic Monitoring System or the casino operator's processes which alter the risk profile of the system;
b) Be approved by management and communicated to all casino operator employees and relevant third-party service provider employees; and
c) Delineate the security roles and responsibilities of casino operator employees and relevant third-party service provider employees for the operation, service and maintenance of the Electronic Monitoring System and/or its components;

B.2.3 ***Access Control Policy.***

An access control policy shall be established and documented within the ISMS which shall be periodically reviewed based on business and security requirements for physical and logical access to the Electronic Monitoring System and/or its components.

a) A formal user registration and de-registration procedure shall be in place for granting and revoking access to the Electronic Monitoring System and/or its components;
b) The allocation of access privileges shall be restricted and controlled based on business requirements and the principle of least privilege;
c) Employees shall only be provided with access to the services or facilities that they have been specifically authorised to use;
d) Employees shall receive appropriate security awareness training and regular updates in organizational policies and procedures as needed for their job function;
e) Management shall review user access rights at regular intervals using a formal process; and
f) The access rights of employees to the Electronic Monitoring System and/or its components shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

B.2.4 ***Allocation of Security Responsibilities.***

Security responsibilities shall be effectively documented and implemented within the ISMS.

a) A security forum comprised of management shall be formally established to monitor and review the ISMS to ensure its continuing suitability, adequacy and effectiveness, maintain formal minutes of meetings, and convene periodically as required by the Commission.
b) A security department shall exist that will be responsible to develop and implement security strategies and action plans. The security department shall:
    i. Be involved in and review all processes regarding security aspects of the casino operator, including, but not be limited to, the protection of information, communications, physical infrastructure, and gaming processes;
    ii. Report to no lower than executive level management and not reside within or report to the IT department; and
    iii. Have the competences and be sufficiently empowered and have access to all necessary resources to enable the adequate assessment, management, and reduction of risk.
c) The head of the security department shall be a member of the security forum and be responsible for recommending security policies and changes.

B.2.5 ***Incident Management.***

A process for reporting information security incidents and the management response shall be documented and implemented within the ISMS in accordance with the information security policy. The incident management process shall:

a) Include a definition of what constitutes an information security incident;
b) Document how information security incidents are reported through appropriate management channels;
c) Address management responsibilities and procedures to ensure a rapid, effective and orderly response to information security incidents, including:
    i. Procedures to handle different types of information security incident;
    ii. Procedures for the analysis and identification of the cause of the incident;
    iii. Communication with those affected by the incident;
    iv. Reporting of the incident to the appropriate authority;
    v. Forensic evidence collection; and
    vi. Controlled recovery from information security incidents.

B.3 Cloud Services

B.3.1 ***Cloud Service Provider Audit.***

A casino operator making use of a cloud service provider, to store, transmit or process personal identification information (PII) and other sensitive information shall undergo a specific audit as required by the Commission. The cloud service provider's operations shall be reviewed against common information security principles in relation to the provision and use of cloud services, as covered within the appendix for "Operational Audit for Technical Security Controls", and this section. It may be acceptable to leverage the results of prior audits conducted by appropriately accredited vendors and qualified individuals, within the current audit period (e.g., within the past year), against standards such as ISO/IEC 27017 and ISO/IEC 27018 or equivalent. Such leveraging will be noted in the audit report.

B.3.2 ***Cloud Service Provider Relationship.***

Cloud security is a shared responsibility between the cloud service provider and the casino operator.

a) If PII and other sensitive information is stored, processed or transmitted in a cloud environment, the applicable requirements will apply to that environment, and will typically involve validation of both the cloud service provider's infrastructure and the casino operator's usage of that environment;
b) The allocation of responsibility between the cloud service provider and the casino operator for managing security controls does not exempt a casino operator from the responsibly of ensuring that PII and other sensitive information is properly secured according to the applicable requirements; and
c) Clear policies and procedures shall be agreed between the cloud service provider and the casino operator for all security requirements, and responsibilities for operation, management and reporting shall be clearly defined and understood for each applicable requirement.

B.4 Gaming Area Services

B.4.1 ***Gaming Area Verification Audit.***

The gaming area will be required to meet the applicable aspects of the appropriate policy and/or procedure documents as determined by the casino operator and approved by the Commission. To maintain the integrity of gaming operations, gaming areas may be subject to an additional verification audit as required by the Commission.

B.4.2 ***Gaming Equipment.***

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

a) 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 unauthorised access;
    iii. Power failures; and
    iv. Other disruptions caused by failures in supporting utilities.
c) Access to the gaming equipment by an employee shall be controlled by a secure logon procedure or other secure process approved by the Commission to ensure that only authorised employees are allowed access. It shall not be possible to modify the configuration settings of the gaming equipment without an authorised secure process;
d) A user session, where supported by gaming equipment, is initiated by the employee logging in to their user account using their secure username and password or an alternative means for the employee to provide identification information as approved by the Commission:
    i. All available options presented to the employee shall be tied to their user account; and
    ii. If the gaming equipment does not receive input from the employee within 5 minutes, or a period specified by the Commission, the user session shall

time out or lock up, requiring the employee to re-establish their login in order to continue.

e) To ensure its continued availability and integrity, 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; and

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

B.4.3 ***Gaming Operations.***

Pursuant to regulation 224(2), the casino operator shall ensure that a key employee or supervisory employee in the gaming department is on the casino premises and responsible for the book at all times during which the licensee is accepting wagers. In addition, the following procedures shall be in place for gaming operations within the gaming area:

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

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

c) Procedures to describe the operations and the servicing of gaming equipment, including the handling of error conditions and performing reconciliations;

d) Procedures to ensure accessibility procedures approved by the Commission are met for the installation of gaming machines.

B.4.4 ***Surveillance and Recording.***

The casino operator 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 gaming information. Procedures shall be in place to ensure that the recording:

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

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

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 houses critical network or system infrastructure.

Act – The Gaming Act, 2014.

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.

Approved Gaming Business – is a “casino operator” as defined in the Act

ARP, *Address Resolution Protocol* – The protocol used to translate IP addresses into MAC addresses to support communication on a wireless or wired local area network.

Audit Trail – A record showing who has accessed a system and what operations the user has performed during a given period.

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. An example is a barcode found on printed gaming tickets.

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.

Bet – Any commitment of credits or money by the patron on the results of events.

Biometrics – A biological identification input, such as fingerprints or retina patterns.

Bonusing Award – An incentive award based on a bet event or some external trigger which do not include triggers based upon specific patron account activity. Examples include multiplied awards, which multiplies all wins within a specified range by a specified value or an nth bet award is won when a total bet on participating events reaches a randomly selected value.

Cache Poisoning – An attack where the attacker inserts corrupt data into the cache database of the Domain Name Service (DNS).

Casino – Any premises, or part of premises, within a designated site where persons may participate in one or more games approved by the Commission under section 91 of the Act.

Casino Employee – An employee having functions in or in relation to a casino.

Casino Operator – A person who is the holder of a casino license. A casino operator whose casino licence permits gaming and operates an Electronic Monitoring System, using both the technological capabilities of the Electronic Monitoring System as well as their own internal procedures.

Commission – The Bermuda Gaming Commission (BGC) established under section 6 of the Act.

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.

Contingency Plan – Management policy and procedures designed to maintain or restore gaming operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

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

Critical Component – Any sub-system for which failure or compromise can lead to loss of patron entitlements, government revenue or unauthorised access to data used for generating reports which are submitted to or reviewed by the Commission. Examples of critical components include— Components which record, store, process, share, transmit or retrieve PII and other sensitive information (e.g., key data, validation numbers, authentication credentials, etc.); Components which generate, transmit, or process random numbers used to determine the outcome of virtual events; Components which store results or the current state of a patron's bet; Points of entry to and exit from the above components (other systems which communicate directly with core critical systems); and Communication networks which transmit sensitive information.

Critical Control Programme – A software programme that controls behaviors relative to any applicable equipment standard and/or regulatory requirement.

Data Integrity – The property that data is both accurate and consistent and has not been altered in an unauthorised manner in storage, during processing, and while in transit.

DDOS, *Distributed Denial of Service* – A type of attack where multiple compromised systems, usually infected with a destructive software program, are used to target a single system. Victims of a DDOS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.

Debit Instrument – A card, code, or other device with which a person may initiate an electronic funds transfer. The term includes, without limitation, a prepaid access instrument.

DNS, *Domain Name Service* – The globally distributed internet database which (amongst other things) maps machine names to IP numbers and vice-versa.

Domain – A group of computers and devices on a network that are administered as a unit with common rules and procedures.

DRP, *Disaster Recovery Plan* – A plan for processing critical applications and preventing loss of data in the event of a major hardware or software failure or destruction of facilities.

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.

eGaming – Gaming or betting in which persons participate by the use of remote communication.

Electronic Monitoring System – means any electronic or computer or communications system or device that is so designed that it may be used, or adapted, to send or receive data from gaming equipment in relation to the security, accounting or operation of gaming equipment.

Encryption – The conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorised people.

Encryption Key – A cryptographic key that has been encrypted in order to disguise the value of the underlying plaintext.

Event – Occurrence related to sports, competitions, matches, and other types of activities approved by the Commission on which bets may be placed.

External Gaming System – System hardware and software separate from that which comprises the Electronic Monitoring System, which may drive the features common to bet offerings, bet configurations, reporting, etc. The patron initially communicates directly with the Electronic Monitoring System which can be integrated with one or more External Gaming Systems.

Firewall – A component of a computer system or network that is designed to block unauthorised access or traffic while still permitting outward communication.

Gaming Area – means the area or areas within the casino premises in which physical gaming, betting and eGaming may take place.

Gaming Software – The software used to take part in gaming and financial transactions with the Electronic Monitoring System which, based on design, is downloaded to or installed on the Gaming Terminal, run from the Electronic Monitoring System which is accessed by the Gaming Terminal, or a combination of the two. Examples of Gaming Software include proprietary download software packages, html, flash, etc.

Gaming Terminal – An electronic device that converts communications from the Electronic Monitoring System into a human interpretable form and converts human decisions into communication format understood by the Electronic Monitoring System.

Gaming Ticket – A printed ticket or electronic message confirming the acceptance of one or more bets.

Group Membership – A method of organizing user accounts into a single unit (by job position) whereby access to system functions may be modified at the unit level and the changes take effect for all user accounts assigned to the unit.

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

HTTP, *Hypertext Transport Protocol* – The underlying protocol used to define how messages are formatted and transmitted, and what actions servers and browsers shall take in response to various commands.

IDS/IPS, *Intrusion Detection System/Intrusion Prevention System* – A system that inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. Used in computer security, intrusion detection refers to the process of monitoring computer and network activities and analyzing those events to look for signs of intrusion in your system.

Incentive Credits and/or Prizes (aka "Incentive Awards") – Credits and/or prizes that is based upon predetermined events or criteria established by the parameters of the Electronic Monitoring System. An incentive award may be a promotional award or a bonusing award.

Information Security – Protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability

Information Security Service Provider – An entity who provides management, support, security, or disaster recovery services for regulated hardware or software.

Internal Control Document – A document that specifies ithe operator's internal control system.

Internal Control System – The system of internal controls that it is required to implement and maintain in relation to its gaming operations, under section 130(1) of the Act.

Internal Controls – The controls, policies, rules, procedures and processes for the operations of a casino.

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

IP Address, *Internet Protocol Address* – A unique number for a computer that is used to determine where messages transmitted on the Internet should be delivered. The IP address is analogous to a house number for ordinary postal mail.

ISMS, *Information Security Management System* – A defined, documented management system that consists of a set of policies, processes, and systems to

manage risks to organizational data, with the objective of ensuring acceptable levels of information security risk.

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

Key Data – Information relating to account balances, personal identification information (PII) and transactional information.

Key Employee – A person in a key employee position.

Key Management – Activities involving the handling of cryptographic keys and other related security parameters (e.g., passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.

Message Authentication – A security measure designed to establish the authenticity of a message by means of an authenticator within the transmission derived from certain predetermined elements of the message itself.

Mobile Code – Executable code that moves from computer to computer, including both legitimate code and malicious code such as computer viruses.

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).

Password – A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorisation.

Patron Account – An account to the credit of a patron for purposes of gaming in a casino whether it is a credit account, a cheque cashing account, a deposit account or any other account opened by or on behalf of a patron with a casino operator.

Patron Account Credit – Credit that is granted by a casino operator to the holder of a patron account and can be drawn on only through the patron account.

PII, *Personal Identification Information* – Key data that could potentially be used to identify a particular patron. 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.

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

Port – A physical entry or exit point of a module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire).

Printer – A Gaming Terminal peripheral that prints gaming tickets and/or wagering instruments.

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

Proxy – An application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. This effectively closes the straight path between the internal and external networks. Making it more difficult for an attacker to obtain internal addresses and other details of the internal network.

Regulations – The Gaming (Casino) Regulations, 2018.

Remote Access – Any access from outside the system or system network including any access from other networks within the same site or casino.

Remote Patron Device – A patron-owned device that at a minimum will be used for the execution or formalization of bets placed by a patron directly. Examples of a Remote Patron Device include a personal computer, mobile phone, tablet, etc.

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

Secure Communication Protocol – A communication protocol that provides the appropriate confidentiality, authentication and content integrity protection.

Security Certificate – Information, often stored as a text file that is used by the Transport Socket Layer (TSL) Protocol to establish a secure connection. In order for an TSL connection to be created, both sides shall have a valid Security Certificate.

Security Policy – A document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance.

Sensitive Information – Includes information such as PINs, key data, passwords, secure seeds and keys, and other data that shall be handled in a secure manner.

Server – A running instance of software that is capable of accepting requests from clients, and the computer that executes such software. Servers operate within a Client-Server Architecture, in which "servers" are computer programs running to serve the requests of other programs ("clients"). In this case the "server" would be the Electronic Monitoring System and the "clients" would be the Remote Patron Devices.

Shellcode – A small piece of code used as a payload in the exploitation of security. Shellcode exploits vulnerability and allows an attacker the ability to reduce a system's information assurance.

Source Code – A text listing of commands to be compiled or assembled into an executable computer program.

Stateless Protocol – A communications scheme that treats each request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of requests and responses.

System Administrator – The individual(s) responsible for maintaining the stable operation of the Electronic Monitoring System (including software and hardware infrastructure and application software).

TCP/IP, *Transmission Control Protocol/Internet Protocol* – The suite of communications protocols used to connect hosts on the Internet.

Testing Laboratory – means a laboratory contracted by the Commission for the purposes of determining the suitability of gaming equipment.

Third-Party Service Provider – An entity who acts on behalf of a casino operator to provide services used for the overall conduct of gaming.

Threat – Any circumstance or event with the potential to adversely impact network operations (including mission, functions, image, or reputation), assets, or individuals

through a system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a system vulnerability.

Time Stamp – A record of the current value of the Electronic Monitoring 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 user input device by using electrical touch point locations on the display screen.

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

User Interface – An interface application or programme through which the user views and/or interacts with the Gaming Software to communicate their actions to the Electronic Monitoring System.

Version Control – The method by which an evolving approved Electronic Monitoring System is verified to be operating in an approved state.

Virus – A self-replicating program, typically with malicious intent, that runs and spreads by modifying other programs or files.

Voucher – A wagering instrument which can be redeemed for cash or used to subsequently redeem for credits.

VPN, *Virtual Private Network* – A logical network that is established over an existing physical network and which typically does not include every node present on the physical network.

Vulnerability – Software, hardware, or other weaknesses in a network or system that can provide a “door” to introducing a threat.

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 patron's mobile device and the Gaming Terminal 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.