GAMING LABORATORIES INTERNATIONAL®

GLI STANDARD SERIES

GLI-16:

STANDARDS FOR CASHLESS SYSTEMS AND TECHNOLOGIES

VERSION: 3.0 DRAFT

REVISION DATE: APRIL 17, 2024

GLI®

WWW.GAMINGLABS.COM

About This Standard

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

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

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

GLI-16 should be viewed as a living document that provides a level of guidance that will be tailored periodically to align with this developing industry over time as gaming implementations and operations evolve.

Table of Contents

Chapter 1: Introduction to Cashless Systems and Technologies

1.1 Introduction

1.1.1 General Statement

Gaming Laboratories International, LLC (GLI) has been testing gaming equipment since 1989. Over the years, GLI has developed numerous technical standards utilized by jurisdictions all over the world. This document, *GLI-16*, sets forth the technical standards for Cashless Systems and Technologies.

1.1.2 Document History

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

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

1.1.3 Acknowledgment of Other Standards Reviewed

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

1.2 Purpose of Technical Standards

1.2.1 General Statement

The purpose of this technical standard is as follows:

a) To eliminate subjective criteria in the evaluation and certification of Cashless Systems and Technologies.
b) To assess the criteria that impacts the credibility and integrity of gaming from both revenue

collection and player perspectives.

c) To establish a standard that will ensure gaming is fair, secure, auditable, and able to be operated correctly.

d) To distinguish between local public policies and Independent Test Laboratory criteria, acknowledging that it is the prerogative of each regulatory body to set its own public policies with respect to gaming.

e) To recognize that the evaluation of internal controls (such as anti-money laundering, financial, and business processes) employed by operators should not be incorporated into the laboratory testing of the standard. Instead, these should be addressed within operational audits performed for local jurisdictions.

f) To develop a standard that can be easily revised to allow for new technology.

g) To formulate a standard that does not specify any particular design, method, or algorithm, thereby allowing a wide range of methods to conform to the standards while simultaneously encouraging the development of new methods.

1.2.2 No Limitation of Technology

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

1.2.3 Adoption and Observance

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

1.3 Other Documents That May Apply

1.3.1 Other GLI Standards

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

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

1.3.2 Minimum Internal Control Standards (MICS)

Implementing Cashless Systems and Technologies is a complex endeavor, necessitating the development of internal processes and procedures to ensure the cashless environment is secure and controlled adequately. To that end, it is expected that a set of Minimum Internal Control Standards (MICS) will be established to define the internal processes for the management and handling of cashless transactions as well as the requirements for internal control of any system or component software and hardware, and their associated accounts.

1.3.3 Gaming Security Framework (GSF)

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

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

1.4 Interpretation of this Document

1.4.1 General Statement

This technical standard applies to Gaming Systems and technologies which allow players to participate in cashless gaming activities using an approved, securely protected authentication method, which accesses:

a) A player account at the Cashless System of the operator; or
b) A player's electronic payment account, provided that it allows for the identification of the account and the source of funds.

NOTE: The intent is to provide a framework to cover payment methods currently known and permitted by law.
NOTE: This technical standard does NOT apply to systems and technologies related to the issuance and redemption of wagering instruments (vouchers and/or coupons) or promotional accounts. For detailed standards applicable to these systems, please reference the *GLI-13 Standards for Monitoring and Control Systems and Voucher Systems* and *GLI-18 Standards for Promotional Systems* as necessary.
NOTE: Cashless Systems which support promotional credits associated with player accounts shall meet the *GLI-18 Standards for Promotional Systems* in addition to this document.
NOTE: This document is not intended to define which parties are responsible for meeting the requirements detailed herein. It is the responsibility of the stakeholders of each jurisdiction to determine how to best meet the requirements laid out in this document.

1.4.2 Software Suppliers and Operators

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

a) Cashless Systems and Technologies may be developed to have configurable features; the final configuration of which depends on the options chosen by the operator. From a testing perspective, it might not be possible to test all of the configurable features of a cashless environment submitted by a software supplier in the absence of the final configuration chosen by the operator; however, the configuration that will be utilized in the production environment shall be communicated to the independent test laboratory to facilitate creating a functionally equivalent test environment.

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

1.5 Testing and Auditing

1.5.1 Laboratory Testing

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

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

1.5.2 Operational Audits

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

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

Chapter 2: Cashless System Requirements

2.1 Introduction

2.1.1 General Statement

A Cashless System may be entirely integrated into an existing Gaming System, such as a Monitoring and Control System, or exist as an entirely separate Gaming System. If the Cashless 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 Cashless 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 Cashless System shall be equipped with a mechanism to ensure the time and dates between all components that comprise the system are synchronized and set correctly.

2.3 Control Program Requirements

2.3.1 Control Program Self-Verification

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

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

2.3.2 Control Program Independent Verification

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

2.4 Critical Components and Functions

2.4.1 Communications

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

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

2.4.2 Servers and Databases

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

2.4.3 Front-End Processor and Data Collectors

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

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

2.4.4 Workstations

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

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

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

2.4.5 Cashless Device Identification

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

2.4.6 Communication Loss Alerts

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

2.4.7 Cashless Device Monitoring

The Cashless System shall be equipped to correctly read and store the applicable significant events and cashless transactions information, and specific cashless meter values from the Cashless Devices, according to the secure communication protocol implemented.

2.4.8 Transaction Communications

The Cashless System shall process cashless transactions correctly according to the secure communication protocol implemented.

2.5 Information to be Maintained

2.5.1 Data Retention and Time Stamping

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

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

2.5.2 System Significant Event Information

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

a) Failed user account access attempts, including IP Address;
b) Program error or authentication mismatch;
c) Significant periods of unavailability of any critical component of the system (e.g., communications are halted and/or system functions cannot be successfully completed for any user);
d) System voids, overrides, and corrections;
e) Changes to live data files occurring outside of normal program and operating system execution;
f) Changes that are made to the download data library, including the addition, changing or deletion of software, where supported;
g) Changes to policies and parameters for operating systems, databases, networks, and applications (e.g., audit settings, password complexity settings, system security levels, manual updates to databases, etc.);
h) Changes to date/time on master time server;
i) For Cashless Systems which support player account management:
    i. Adjustments to a player account balance;
    ii. Changes made to sensitive information recorded in a player account;
    iii. Suspension or closure of a player account;
    iv. Large financial transactions (single and aggregate over defined time period) in excess of a value specified by the regulatory body, including transaction information;
    v. Negative player account balance (due to adjustments and/or chargebacks);
j) Large cashless transactions (single and aggregate over defined time period) in excess of a value specified by the regulatory body, including transaction information;
k) Irrecoverable loss of sensitive information;
l) Any other activity requiring user intervention and occurring outside of the normal scope of system operation; and
m) Other significant or unusual events as deemed applicable by the regulatory body.

2.5.3 User Account Information

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

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

2.5.4 Cashless Transaction Information

The information to be maintained and backed up for each cashless transaction at a Cashless Device shall include, as applicable:

a) The type of transaction (e.g., transfer to/from Cashless Device, etc.);
b) The date and time of the transaction;
c) Unique transaction ID;
d) Amount of transaction;
e) Transaction status (pending, complete, etc.);
f) Unique Cashless Device ID or equivalent which handled the transaction; and
g) Unique player account ID, or for electronic payment accounts, an identifier which can be used to authenticate the type of account and the source of the funds (i.e. source of where funds came from/went to).

2.5.5 Player Account Information

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

a) Unique player account ID and username (if different);
b) For player accounts which are registered to a player:
   i. The personally identifiable information (PII) collected by the operator to register a player and create the account, including, the legal name, date of birth, residential address, and contact information;
   ii. The player's government identification number (social security number, taxpayer identification number, passport number, or equivalent), authentication credentials, and personal financial information (debit instrument numbers, credit card numbers, bank account numbers, etc.), which shall be encrypted or hashed to a cryptographic algorithm as allowed by the regulatory body;
   iii. The date and method of identity verification, including, where applicable, a description of the identification credential provided by a player to confirm their identity and its date of expiration;
   iv. Previous accounts, if any, and reason for closure;
c) The date of player agreement to the operator's terms and conditions and privacy policy;

d) Account details and current balance. All discretionary account funds shall be maintained separately;
e) The date and method from which the account was opened (e.g., remote vs. on-site), including relevant location information;
f) The date and time of account is accessed by any person (player or operator), including relevant location information;
g) Where supported, exclusions/limitations information as required by the regulatory body:
    i. The date and time of the request;
    ii. Description and reason of exclusion/limitation;
    iii. The type of exclusion/limitation (e.g., system-imposed deposit limitation, self-imposed deposit limitation, self-imposed temporary exclusion);
    iv. The date exclusion/limitation commenced;
    v. The date exclusion/limitation ended;
h) Financial transaction information:
    i. The type of transaction (e.g., deposit, withdrawal, adjustment, etc.);
    ii. The date and time of the transaction;
    iii. Unique transaction ID;
    iv. Amount of transaction;
    v. Total account balance before/after transaction;
    vi. Total amount of fees paid for transaction, if any;
    vii. Unique Cashless Device ID or equivalent which handled the transaction;
    viii. Transaction status (pending, complete, etc.);
    ix. Method of deposit/withdrawal (e.g., cash, personal check, cashier's check, wire transfer, money order, debit instrument, credit card, electronic funds transfer, etc.);
    x. Deposit authorization number;
    xi. Relevant location information.
i) The current status of the player account (e.g., active, inactive, closed, excluded, etc.).

NOTE: For information above that is not maintained directly by the system, internal controls may be in place to ensure this information is recorded.

2.6 Reporting Requirements

2.6.1 General Reporting Requirements

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

a) These required reports shall be able to be produced on demand, on a daily basis, and for other intervals required by the regulatory body (e.g., month-to-date (MTD), year-to-date (YTD), life-to-date (LTD), etc.).
b) Each required report shall contain:
    i. The operator's name (or other identifier), the title of report, the selected interval and the date/time the report was generated;

ii. An indication of “No Activity” or similar message if no information appears for the period specified; and
iii. Labeled fields which can be clearly understood in accordance with their function.

2.6.2 System Significant Events and Alterations Reports

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

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

2.6.3 Player Account Reports

For Cashless Systems which support player account management, the following reports shall be able to be produced for player accounts, as applicable:

a) Player Account Activity Reports. These reports are to include, for each player account, balance, deposit and withdrawal amounts, transfers to and from Cashless Devices, and adjustments (single transaction amounts and aggregate amounts); and
b) Player Account Liability Reports. These reports are to include, for each gaming day, the starting liability amount (total amount held by the operator for player accounts), total additions and subtractions to account balances, and the ending liability.

2.6.4 Meter Reconciliation Reports

The following information shall be provided to produce one or more reports for reconciling each Cashless Device’s metered amounts against the Cashless System’s recorded amounts, as applicable:

a) Unique Cashless Device ID or equivalent;
b) Electronic Funds Transfer In (EFT In) meter vs. system recorded EFT In transactions;
c) Player Account Transfer In (WAT In) meter vs. system recorded WAT In transactions;
d) Player Account Transfer Out (WAT Out) meter vs. system recorded WAT Out In transactions; and
e) Any other information needed for reconciliation which is not covered by the above.

2.6.5 Cashier Summary and Detail Reports

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

a) Unique Cashier Station ID or equivalent;
b) User account ID or name of cashier;

c) The date and time the cashier session began;
d) The cashier balances at the start and end of the cashier session;
e) For each financial transaction:
   i. Unique transaction ID;
   ii. Unique player account ID;
   iii. The type of transaction (e.g., deposit, withdrawal, adjustment, etc.);
   iv. The transaction value in local monetary units in numerical form;
   v. The date and time of the transaction; and
f) The cashier balance at the end of the cashier session (blank until known).

Chapter 3: Cashless Device Requirements

3.1 Introduction

3.1.1 General Statement

The requirements throughout this chapter apply to kiosks, gaming devices, electronic table games, electronic wager stations, live game management components, and any other critical gaming equipment maintained by the operator and used in the cashless environment, also known as Cashless Devices. Any additional device or software which is used to meet a regulatory requirement may also be subject to these requirements based on functionality.

3.2 Device Requirements

3.2.1 Identifying a Cashless Device

A player should be able to identify each Cashless Device by a means left to the discretion of the individual regulatory body (e.g. remove display menu items that pertain to cashless functionality for gaming equipment not participating; provide a host message indicating cashless capability; or a specific sticker on the gaming equipment to indicate participation or non-participation).

3.2.2 Configuring Cashless Transactions

Since cashless functionality would impact the electronic accounting meters, it shall not be possible to change a configuration setting that causes any obstruction or alteration to these meters without performing an NV memory clear.

3.2.3 Diagnostic Tests on a Cashless Device

Controls shall be in place for any diagnostic functionality available at the Cashless Device such that all activity shall be reported to the Cashless System that would reflect the specific account(s) and the individual(s) tasked to perform these diagnostics. This would allow all cashless diagnostic activity that affects the Cashless Device's associated electronic accounting meters to be audited.

3.3 Player Identification Components

3.3.1 General Statement

A player identification component is software and/or hardware used with a Cashless Device which supports a means for players to provide identification information and/or the source of funds. This includes components which are controlled by a Cashless Device's critical control program and interface element-based or non-integrated form of these components that operate outside the control of the Cashless Device. Examples of these components include card readers, barcode readers, and biometric scanners.

3.3.2 General Component Requirements

Player identification components shall be constructed in a manner that ensures proper handling of inputs and that protects against vandalism, abuse, or fraudulent activity. In addition, player identification components shall meet the following rules:

a) The player identification component shall be designed to prevent manipulation that may impact integrity and shall provide a method to enable the software to interpret and act appropriately upon a valid or invalid input;
b) Acceptance of any identification information shall only be possible when the Cashless Device is enabled for use. Other states, such as error conditions including door opens, shall cause the disabling of the player identification component; and
c) Any player identification component which locally stores information relating to cashless transactions shall not have means to compromise such information and shall not allow the removal of its information until that information has been successfully transferred and acknowledged by the Cashless System.

3.3.3 Card Readers

Card reader software shall be able to detect the use of a valid card, as applicable. The card reader shall be electronically based and be configured to ensure that it only reads valid cards.

3.3.4 Barcode Readers

Barcode reader software shall be able to associate the barcode or any machine-readable code visible on a card or an allowed software application on a player's mobile device (such as a smartphone or tablet), as applicable, with data stored in an external database as a means to identify and validate an account association, or for the purpose of redemption.

3.3.5 Biometric Scanners

Biometric scanner software shall be able to associate a person's physical characteristics with those recorded within an external database as means to authenticate the identity of a player and for the purpose of account association.

3.3.6 Wireless Devices

Software which controls communication between a Cashless Device and any wireless devices that are conducted using contactless transmission technologies such as Near Field Communications (NFC), Bluetooth (BT), Wi-Fi, optical, etc., shall:

a) Utilize secure communication methods to prevent unauthorized access to sensitive information by unintended recipients;
b) Employ a method to detect data corruption; upon detection of corruption, either correct the error, or terminate the communication while providing a suitable error message;

c) Employ a method to prevent unauthorized modification of sensitive information that impacts device integrity or that represents secure player data; and
d) Only be possible with authorized player identification components.

NOTE: The independent test laboratory will make every attempt to ensure secure communications are employed and document attempts to intervene on communications.

3.3.7 Smart Card/Device Technology

If allowed by the regulatory body, players may access their accounts using smart card/device technology, including smartphone and tablet technology where the account information, including the current account balance, is maintained in the Cashless System's database. Smart cards/devices which have the ability to maintain a player account balance are only permissible when the Cashless System validates that the amount on the card/device agrees with the amount stored within the system's database (i.e., smart cards/devices cannot maintain the only source of account data).

NOTE: Smart card/device technology implementation will be evaluated on a case-by-case basis.

3.3.8 Hardware Location

The player identification component hardware shall be secured in a locked enclosure or sealed casing or located within a locked area of the Cashless Device outside of any logic areas (i.e., an area that requires opening of the main door for access). Only the areas of the component that require physical interaction shall be accessible to the player.

3.3.9 Error Conditions

The Cashless Device shall have mechanisms to interpret and act upon an error condition related to a malfunction of any player identification component, including communication failures. If a player identification component error condition is identified, the Cashless Device shall display an appropriate error message and disable the player identification component. This error condition shall be communicated to the connected system when such a compatible system and protocol is supported.

3.4 Cashless Transactions

3.4.1 Cashless Transaction Authentication

All cashless transactions between a supporting Cashless Device and the Cashless System shall be secured using a method of authentication, such as credit or debit instrument, card insertion or "tap" (contactless) capacity on the player identification component, a similar approved process that allows for the identification of the account and the source of funds if a software application on a player's mobile device is used, or a secure alternative means (e.g. finger-print recognition). Authentication methods are subject to the discretion of the regulatory body as necessary. The requirement does not prohibit the option for more than one method of authentication being available for a player to access their account. Cashless transactions are entirely electronic.

a) An explanatory message shall be displayed to the player if there is an identification failure (e.g., account is not recognized, invalid PIN, etc.).
b) Current account balance information shall be available to the player once authenticated. All discretionary account funds shall be indicated separately.

3.4.2 Player Account Transfers

After the player's identity is confirmed, any available transfer options for their player account shall be made available to the player, which will require selection before occurring.

a) Players may have the option of moving some or all of their account balance to the Cashless Device's credit meter through a "download" or "withdrawal" from the player account. Some systems may move either a predefined amount or the player's entire account balance to the Cashless Device for play;
b) A transfer shall not be accepted that could cause the player to have a negative balance;
c) The account balance is to be debited when the transfer is accepted by the Cashless System and funds are added to the Cashless Device's credit meter;
d) Once play is completed, the player may have the option to "upload" or "deposit" their credit meter balance from the Cashless Device onto their player account or cash-out some credits. Some systems may require that the entire credit meter balance be transferred back to the system; and
e) Any credits on the Cashless Device that are attempted to be transferred to the Cashless System that result in a communication failure for which this is the only available payout medium (the player cannot cash-out via voucher issuance or other method), shall result in a handpay lockup or tilt on the Cashless Device.

3.4.3 Direct Account Wagering

If the Cashless Device and the Cashless System support the ability to directly wager from the player account (i.e. credits are not transferred between the player account and the Cashless Device), the following shall apply:

a) A wager shall not be accepted that could cause the player to have a negative balance; and
b) The account balance is to be debited when the wager is accepted by the Cashless System.

3.4.4 Transaction Messages

A confirmation/denial message shall be displayed to the player whenever any cashless transaction is being processed, including:

a) The type of transaction (upload/download);
b) The transaction value; and
c) For denied transactions, a descriptive message as to why the transaction did not complete as initiated.

3.4.5 Transaction Limits

If a player initiates a cashless transaction and that transaction would exceed Cashless Device or System configured limits (i.e. the credit limit, transaction limit, etc.) or any limit that has been established for purposes of responsible gaming then this transaction may only be processed provided that the player is clearly notified that they have transacted less than requested to avoid player disputes.

3.4.6 Credit or Debit Instrument Transactions

In the event of a credit or debit instrument transaction at the Cashless Device, the Cashless System shall:

a) Execute the transaction in accordance with all applicable jurisdictional electronic funds transfer requirements or player account transfer requirements including receipting and fee disclosure requirements; and
b) Not execute a transaction upon notification from the player's financial institution that the available credit or funds associated with the player's credit or debit instrument are less than the amount requested by the player. Alternatively, a transaction of the available credit or funds may be processed provided that the player is clearly notified that they have transacted less than requested.

3.5 Cashless Meters and Logs

3.5.1 Information Access

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

3.5.2 Cashless Meters

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

a) The required electronic accounting meters for each Cashless Device are as follows:
   ii. Electronic Funds Transfer In (EFT In). There shall be a meter that accumulates the total value of cashable player funds electronically transferred to the Cashless Device from a financial institution through a Cashless System or through the secure interface that uses a defined protocol;
   iii. Player Account Transfer In (WAT In). There shall be a meter that accumulates the total value of cashable player funds electronically transferred to the Cashless Device from a player

account through a Cashless System or through the secure interface that uses a defined protocol. This meter does not include transfers of promotional credits;

iv. Player Account Transfer Out (WAT Out). There shall be a meter that accumulates the total value of cashable player funds electronically transferred from the Cashless Device to a player account through a Cashless System or through the secure interface that uses a defined protocol. This meter does not include transfers of promotional credits;

v. Other Meters. Cashless transactions that would not otherwise be metered under any of the above meters, shall be recorded on sufficient meters to properly reconcile all such transactions.

b) The operation of other mandatory meters for Cashless Devices shall not be impacted directly by cashless transactions.

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

3.5.3 Cashless Transaction Log

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

a) The type of transaction (upload/download);
b) The transaction value in local monetary units in numerical form;
c) The time of day of the transaction, in twenty-four (24) hour format showing hours and minutes;
d) The date of the transaction, in any recognized format, indicating the day, month, and year; and
e) Unique player account ID, or for electronic payment accounts, an identifier which can be used to authenticate the type of account and the source of the funds (i.e. source of where funds came from/went to) where only the last four (4) digits may be displayed by the Cashless Device.

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

3.6 System Communication Requirements

3.6.1 Interface Elements

Where Cashless Devices use interface elements to communicate with the Cashless System, the interface elements shall meet the applicable “Interface Element Requirements” within the *GLI-13 Standards for Monitoring and Control Systems and Validation Systems* and/or other applicable jurisdictional requirements observed by the regulatory body.

3.6.2 Protection of Sensitive Information

The Cashless Device shall not allow any sensitive information contained in communication to or from the Cashless System that are intended by the secure communication protocol to be protected, to be viewable through any display mechanism supported by the device.

3.6.3 Loss of Communication

If communication with the Cashless System is lost, the Cashless Device shall cease operations related to that communication, and a message shall be displayed to the player that cashless transactions cannot currently be processed. It is permissible for the Cashless Device to detect this error when the device tries to communicate with the system.

Chapter 4: Player Account Requirements

4.1 Introduction

4.1.1 General Statement

The requirements of this chapter apply to player accounts where supported by the Cashless System and maintained by the operator. This chapter does not apply to electronic payment accounts.

4.2 Player Account Management

4.2.1 Registered Player Account Registration and Verification

For player accounts which are registered to a player, there shall be a method to collect their personally identifiable information (PII) as a part of the registration process. Where player account registration and verification are supported directly by the Cashless System, the following requirements shall be met:

a) Only players of the legal gaming age for the jurisdiction may register for a player account. During the registration process, the player shall:
   i. Be denied the ability to register for a player account if they submit a birth date which indicates that they are underage;
   ii. Be informed on the registration form which information fields are “required”, which are not, and what will be the consequences of not filling in the required fields;
   iii. Agree to the terms and conditions and privacy policy:
   iv. Acknowledge that they are prohibited from allowing any unauthorized person to access or use their player account;
   v. Consent to the monitoring and recording of the use of their player account by the operator and the regulatory body; and
   vi. Affirm that the PII the player is providing to open the player account is accurate.

b) Identity verification shall be undertaken before a player is allowed to play a game. Third-party identity verification service providers may be used for identity verification as allowed by the regulatory body.
   i. Identity verification shall authenticate the legal name, date of birth and government identification number (social security number, taxpayer identification number, passport number, or equivalent) of the individual at a minimum as required by the regulatory body.
   ii. Identity verification shall also confirm that the player is not on any exclusion lists held by the operator or the regulatory body or prohibited from establishing or maintaining an account for any other reason.
   iii. Details of identity verification shall be kept in a secure manner.

c) The player account can only become active once age and identity verification are successfully completed, the player is determined to not be on any exclusion lists or prohibited from establishing or maintaining an account for any other reason, the player has acknowledged the necessary terms and conditions and privacy policy, and the player account registration is complete.

d) A player shall only be permitted to have one active player account at a time unless specifically authorized by the regulatory body.
e) The system shall allow the ability to view and update authentication credentials, registration information and the account used for financial transactions for each player. A multi-factor authentication process shall be employed for these purposes.

4.2.2 Anonymous Player Account Balance Limits

Where allowed by the regulatory body, anonymous player accounts may be used where supported by the Cashless System. Where required by the regulatory body, the Cashless System shall enforce a maximum balance limit on the anonymous player account.

a) Deposits may not occur which cause the player account balance to exceed this limit; and
b) If the player account's balance exceeds this limit due to game play, adjustments, or any other additions to the balance, the system shall then suspend the account from play until the balance is reduced to a value equal to or less than the maximum balance limit at a Kiosk or Cashier Station.

4.2.3 Player Account Access at the System

In addition to the authentication methods mentioned for "Cashless Transaction Authentication", a player account may be accessed at the Cashless System using authentication credentials, such as a username (or similar) and a password or a secure alternative means to perform authentication to log in.

a) If the system does not recognize the authentication credentials provided, an explanatory message shall be displayed. The error message shall be the same regardless of which authentication credential is incorrect.
b) Where a player has forgotten their authentication credentials, a multi-factor authentication process shall be employed for the retrieval or reset of their forgotten authentication credentials.
c) Player accounts are automatically locked-out after three successive failed active access attempts in a thirty-minute period. The system may release a locked-out account after thirty minutes has elapsed. If a gaming attendant assists with releasing a locked-out account and is reasonably certain of no unauthorized access (if such information can be provided by the system and is readily available to the attendant assisting in unlocking the account), the elapsed time of thirty minutes is not required.
d) The system shall support a mechanism that allows for an account to be locked in the event that other suspicious activity is detected. A multi-factor authentication process shall be employed for the account to be unlocked.

4.2.4 Financial Transactions

Funds may be deposited to or withdrawn from the player account via a Cashier Station or any supporting Cashless Device (through coins/tokens, bills, wagering instruments, credit or debit instruments, etc.) or from an approved secure interface that uses a defined protocol or similar software application on a player's mobile device (such as a smartphone or tablet) that complies with the requirements with respect to player identification and source of funds. Where financial transactions can be performed automatically by the Cashless System the following requirements shall be met:

a) The system shall provide confirmation/denial of every financial transaction initiated, including
    i. The type of transaction (deposit/withdrawal);
    ii. The transaction value; and
    iii. For denied transactions, a descriptive message as to why the transaction did not complete as initiated.
b) Funds deposited into a player account shall not be available for wagering until they are received from the issuer or the issuer provides an authorization number indicating that the funds are authorized. The authorization number is to be maintained in an audit log.
c) Where financial transactions are allowed through Electronic Funds Transfers (EFT), there shall be security measures and controls in place to prevent EFT fraud. A failed EFT attempt may not be considered fraudulent if the player has successfully performed an EFT on a previous occasion with no outstanding chargebacks. Otherwise, the player account shall:
    i. Be temporarily blocked for investigation of fraud after five consecutive failed EFT attempts within a ten-minute time period or a period to be determined by the regulatory body. If there is no evidence of fraud, the block may be removed; and
    ii. Have its access suspended after five additional consecutive failed EFT attempts within a ten-minute period or a period to be determined by the regulatory body.
d) Positive player identification or authentication shall be completed before the withdrawal of any funds can be made by the player. Cashless devices that permit players to withdrawal funds without interacting with the operator shall authenticate users using multi-factor authentication.
e) A player account shall not be overdrawn unless caused by payment processing issues outside the control of the system.
f) Payments from an account are to be paid (including funds transfer) directly to an account with a financial institution in the name of the player or made payable to the player and forwarded to the player's address using a secure delivery service or through another method that is not prohibited by the regulatory body. The name and address are to be the same as held in player registration details.
g) If a player initiates a financial transaction and that transaction would exceed limits put in place by the operator and/or regulatory body, this transaction may only be processed provided that the player is clearly notified that they have withdrawn or deposited less than requested.
h) It shall not be possible to transfer funds between two player accounts.
i) Security or authorization procedures shall be in place to ensure that only authorized adjustments can be made to player accounts, and these changes are auditable.

4.2.5 Transaction Log or Account Statement

The Cashless System shall be able to provide a transaction log or account statement history to a player upon request. The information provided shall include sufficient information to allow the player to reconcile the statement or log against their own financial records. Information to be provided shall include at a minimum, details on the following types of cashless and financial transactions (time stamped with a unique transaction ID) within the past year or other time period as requested by the player or as required by the regulatory body:

a) Deposits to the player account;
b) Withdrawals from the player account;
c) Credits added to/removed from the player account from game play;
d) Manual adjustments or modifications to the player account (e.g., due to refunds); and
e) Any other additions to, or deductions from, the player account, that would not otherwise be metered under any of the above-listed items.

4.2.6 Account Closure

Players shall be provided with a method to close their player account at any time unless the operator has temporarily excluded a player from gaming. Any balance remaining in a player account shall be refunded to the player, provided that the operator acknowledges that the funds have cleared.

4.3 Limitations and Exclusions

4.3.1 General Statement

The requirements in this section apply where the Cashless System supports the ability to directly manage and implement limitations and/or exclusions.

4.3.2 Limitations

Players shall be provided with a method to impose limitations for gaming parameters including, but not limited to deposits and cashless transactions as required by the regulatory body. In addition, there shall be a method for the system to impose any limitations for gaming parameters as required by the regulatory body.

a) Once established by a player and implemented by the system, it shall only be possible to reduce the severity of self-imposed limitations upon twenty-four hours' notice, or as required by the regulatory body.
b) Players shall be notified in advance of any system-imposed limits and their effective dates. Once updated, system-imposed limits shall be consistent with what is disclosed to the player.
c) Upon receiving any self-imposed or system-imposed limitation order, the system shall ensure that all specified limits are correctly implemented immediately or at the point in time (e.g., next login, next day) clearly indicated to the player.
d) The self-imposed limitations set by a player shall not override more restrictive system-imposed limitations. The more restrictive limitations shall take priority.
e) Limitations shall not be compromised by internal status events, such as self-imposed exclusion orders and revocations.

4.3.3 Exclusions

Players shall be provided with a method to exclude themselves from access to their player account for a specified period or indefinitely, as required by the regulatory body. In addition, there shall be a method for the operator to exclude a player from access to their player account as required by the regulatory body.

a) Players shall be given a notification containing exclusion status and general instructions for resolution where possible.
b) Immediately upon receiving the exclusion order, no new wagers or deposits are accepted from that player, until the exclusion has been removed.
c) While excluded, the player shall not be prevented from withdrawing any or all of their account balance, provided that the operator acknowledges that the funds have cleared, and that the reason(s) for exclusion would not prohibit a withdrawal.

Appendix A: Internal Controls for Cashless Environments

A.1 Introduction

A.1.1 General Statement

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

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

A.2 Internal Control Procedures

A.2.1 Internal Control Procedures

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

A.2.2 Information Management

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

A.2.3 Risk Management

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

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

A.3 General Operating Procedures

A.3.1 Operator Reserves

The operator shall have processes in place for maintaining and protecting adequate cash reserves, as determined by the regulatory body, including segregated accounts of funds held for player accounts and any operational funds used to cover all other operator liability if defined by the regulatory body.

A.3.2 Protection of Player Funds

The operator shall have processes in place to ensure funds in an operator account are either to be held in trust for the player in a segregated account or in a special purpose segregated account that is maintained and controlled by a properly constituted corporate entity that is not the operator and whose governing board includes one or more corporate directors who are independent of the operator and of any corporation related to or controlled by the operator. In addition, the operator shall have procedures that are reasonably designed to:

a) Ensure that funds generated from gaming are safeguarded and accounted for;
b) Make clear that the funds in the segregated account do not belong to the operator and are not available to creditors other than the player whose funds are being held; and
c) Prevent commingling of funds in the segregated account with other funds including, without limitation, funds of the operator.

A.4 Player Account Controls

A.4.1 Registration and Verification

Where player account registration is done manually by the operator, procedures shall be in place to satisfy the requirements for "Registered Player Account Registration and Verification" as indicated within this document.

A.4.2 Fraudulent Accounts

The operator shall have a documented public policy for the treatment of player accounts discovered to being used in a fraudulent manner, including but not limited to:

a) The maintenance of information about any account's activity, such that if fraudulent activity is detected, the operator has the necessary information to take appropriate action;
b) The suspension of any account discovered to be engaged in fraudulent activity, such as a player providing access to underage persons; and
c) The handling of deposits, wagers, and wins associated with a fraudulent account.

A.4.3 Terms and Conditions

A set of terms and conditions shall be available to the player via external signage, forms, or brochures available at the gaming venue. During the registration process and when any terms and conditions are materially updated (i.e., beyond any grammatical or other minor changes), the player shall agree to the terms and conditions. The terms and conditions shall:

a) Advise the player to keep their authentication credentials (e.g., password and username) secure;
b) Disclose all processes for dealing with lost authentication credentials, forced password changes, password strength and other related items as required by the regulatory body;
c) Specify the conditions under which an account is declared inactive and explain what actions will be undertaken on the account once this declaration is made;
d) Clearly define what happens to the player's wagers placed but remaining undecided in interrupted games prior to any self-imposed or operator-imposed exclusion, including the return of all wagers, or settling all wagers, as appropriate;
e) Contain information about timeframes and limits regarding deposits to and/or withdrawals from the player account, including a clear and concise explanation of all fees (if applicable);
f) State that the operator has the right to:
    i. Refuse to establish a player account for what it deems good and sufficient reason;
    ii. Refuse deposits to and/or withdrawals from player accounts for what it deems good and sufficient reason; and
    iii. Unless there is a pending investigation or player dispute, suspend or close any player account at any time pursuant to the terms and conditions between the operator and the player.

A.4.4 Privacy Policy

A privacy policy shall be available to the player via external signage, forms, or brochures available at the gaming venue. During the registration process and when the privacy policy is materially updated (i.e., beyond any grammatical or other minor changes), the player shall agree to the privacy policy. The privacy policy shall state:

a) The personally identifiable information (PII) required to be collected;
b) The purpose and legal basis for PII collection and of every processing activity for which consent is being sought;
c) The period in which the PII is stored, or, if no period can be possibly set, the criteria used to set this;
d) The conditions under which PII may be disclosed;
e) An affirmation that measures are in place to prevent the unauthorized or unnecessary disclosure of the PII;
f) The identity and contact details on the operator who is seeking the consent, including any third-party service providers which may access and/or use this PII;
g) The rights and possibility of a player to file a complaint to the regulatory body; and
h) For PII collected directly from the player, whether there is a legal or contractual obligation to provide the PII and the consequences of not providing that PII.

A.4.5 Account Sensitive Information Security

Any sensitive information obtained in respect to the player account, including personally identifiable information (PII) and player funds, shall be done in compliance with the privacy policy and local privacy regulations and standards observed by the regulatory body. Sensitive information shall be considered as a critical asset for the purposes of risk assessment.

a) Any sensitive information which is not subject to disclosure pursuant to the privacy policy shall be kept confidential, except where the release of that information is required by law. This includes, but is not limited to:
   i. The amount of money credited to, debited from, or present in any particular player account;
   ii. The amount of money wagered by a particular player on any game;
   iii. The account number and authentication credentials that identify the player; and
   iv. The name, address, and other information in the possession of the operator that would identify the player to anyone other than the regulatory body or the operator.
b) There shall be procedures in place for the security and sharing of sensitive information as required by the regulatory body, including, but not limited to:
   i. The designation and identification of one or more individuals having primary responsibility for the design, implementation and ongoing evaluation of such procedures and practices;
   ii. The procedures to be used to determine the nature and scope of all information collected, the locations in which such information is stored, and the storage devices on which such information may be recorded for purposes of storage or transfer;
   iii. The measures to be utilized to protect information from unauthorized access; and
   iv. The procedures to be used in the event the operator determines that a breach of data security has occurred, including required notification to the regulatory body.

A.4.6 Player Funds Maintenance

Procedures shall be in place to ensure all financial transactions are conducted in accordance with local commerce regulations and requirements mandated by the regulatory body.

a) Where financial transactions cannot be performed automatically by the Cashless System, procedures shall be in place to satisfy the requirements for “Financial Transactions” as indicated within this document.
b) A player’s request for withdrawal of funds (i.e., deposited and cleared funds and wagers won) shall be completed by the operator within a reasonable amount of time, unless there is a pending unresolved player complaint/dispute or investigation. Such investigation shall be documented by the operator and available for review by the regulatory body.

A.4.7 Inactive Accounts

A player account is considered to be inactive under the conditions as specified in the terms and conditions. Procedures shall be in place to:

a) For registered player accounts, allow access by player to their inactive account only after performing additional identity verification;
b) Protect inactive player accounts that contain funds from unauthorized access, changes or removal; and
c) Deal with unclaimed funds from inactive player accounts, including returning any remaining

funds to the player where possible.

A.4.8 Test Accounts

The operator may establish test accounts to be used to test or have tested the various components and operation of a Cashless System in accordance with internal controls adopted by the operator, which, at a minimum, shall address the following procedures:

a) The procedures for authorizing testing activity and assigning each test account for use;
b) The procedures for the issuance of funds used for testing, including the identification of who is authorized to issue the funds and the maximum amount of funds that may be issued;
c) The maintenance of a record for all test accounts, to include when they are active and to whom they are issued; and
d) The procedures for the auditing of testing activity to ensure the accountability of funds used for testing and proper adjustments to reports and records.

A.5 Monitoring Procedures

A.5.1 Anti-Money Laundering (AML) Monitoring

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

a) A system of internal controls to assure ongoing compliance with the local AML regulations and standards observed by the regulatory body;
b) Up to date training of personnel in the identification of unusual or suspicious transactions;
c) Assigning an individual or individuals to be responsible for all areas of AML by the operator including reporting unusual or suspicious transactions;
d) Monitoring applicable Cashless Devices for cashable credits transferred into the Cashless Device from one player account or electronic payment account then transferred out to another account;
e) Monitoring player accounts for opening and closing in short time frames and for deposits and withdrawals without associated game play;
f) Ensuring that aggregate transactions over a defined period may require further due diligence checks and may be reportable to the relevant organization(s) if they exceed the threshold prescribed by the regulatory body;
g) Use of any automated data processing systems to aid in assuring compliance; and
h) Periodic independent tests for compliance with a scope and frequency as required by the regulatory body. Logs of all tests shall be maintained.

Glossary of Key Terms

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

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

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

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

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

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

BT, *Bluetooth* – A low power, short-range wireless communications protocol utilized for the interconnection of cellular phones, computers, and other electronic devices, including Cashless Devices. Bluetooth connections typically operate over distances of 10 meters or less and rely upon short-wavelength radio waves to transmit data over the air.

Card Reader – A device that reads data embedded on a magnetic strip, or stored in an integrated circuit chip, for player identification.

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

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

Cashless Device – An electronic device which facilitates financial transactions with a player account and/or cashless transactions between a player account or electronic payment account and Gaming Equipment maintained by the operator and used in the cashless environment. Any additional device or software which is used to meet a regulatory requirement may also be subject to control based on functionality.

Cashless System – The hardware, software, firmware, communications technology, other equipment, as well as operator procedures implemented in order to allow players to participate in wagering activities using an approved authentication method, which accesses a player account at the

Cashless System of the operator or an electronic payment account of the player provided that it allows for the identification of the account and the source of funds. The system provides the operator with the means to review player accounts, generate various cashless/financial transaction and account reports, and set any configurable parameters.

Cashless Transactions — The electronic transfer to/from a Cashless Device of a player account's funds using a Cashless System. The term also includes electronic funds transferred from an electronic payment account to a Cashless Device.

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.

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

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

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

Discretionary Account Funds – Non-cashable promotional credits and promotional credits that have a possible expiration.

EFT, *Electronic Funds Transfer* (aka "ECT", "Electronic Credits Transfer") — An electronic transfer of funds from an independent financial institution to a player account or Cashless Device through a Cashless System. This includes Automated Clearing House (ACH) transfers.

Electronic Accounting Meter (aka "Software Meter" / "Soft Meter") — An accounting meter that is implemented in Cashless Device software.

Electronic Payment Account — An account maintained with a financial institution or other third-party for purposes of making electronic payments, such as PayPal, Google Pay, or Apple Pay, that is intended for general use and not only for gaming purposes.

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

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

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

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

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

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

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

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

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

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

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

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

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).

NFC, *Near Field Communication* – A short-range wireless connectivity standard that uses magnetic field induction to enable communication between devices when they are touched together or brought within a few centimeters of each other.

Non-Cashable Promotional Credits (aka "Restricted Promotional Credits") – Promotional credits that are not redeemable for cash.

Operator – A person or entity that oversees a cashless environment and/or maintains player accounts using both the technological capabilities of the Cashless System as well as their own internal control procedures.

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

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

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

Player Account (aka "Wagering Account" / "Cashless Account") – An account maintained by an operator for a player where information relative to financial and cashless transactions are recorded on behalf of the player including, but not limited to, deposits, withdrawals, wagers, winnings, and balance adjustments. The term does not include an electronic payment account, or an account used solely by an operator to track promotional points or credits, or similar benefits issued by an operator to a player which may be redeemed for merchandise and/or services.

Player Account Transfer (aka "Wagering Account Transfer" / "Cashless Account Transfer") – Cashable player funds electronically transferred to/from the Cashless Device from a player account.

Player Identification Component – Software and/or hardware used with a Cashless Device which supports a means for players to provide identification information and/or the source of funds. Examples include a card reader, a barcode reader, or a biometric scanner.

Prepaid Access Instrument – A card, code, electronic serial number, mobile identification number, personal identification number or similar device used in conjunction with a Cashless System that allows player access to funds that have been paid in advance and can be retrieved or transferred at some point in the future through such a device.

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

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

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

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

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

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

Smart Card – A card with embedded integrated circuits that possesses the means to electronically store or retrieve account data.

Tilt – An error in Cashless Device operation that halts or suspends operations and/or that generates some intelligent fault message.

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

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

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

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