GLI STANDARD SERIES

GLI-16:

STANDARDS FOR CASHLESS SYSTEMS AND TECHNOLOGIES

VERSION: 3.0

REVISION DATE: JULY 31, 2024

About This Standard

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

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

GLI-16 should be viewed as a living document 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. 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 technical 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 or technology, 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 production environment is secure and controlled adequately. To that end, it is expected that a set of Minimum Internal Control Standards (MICS) will be established by the regulatory body to define the minimum required 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 within the cashless production environment, and their associated accounts. The regulatory body's MICS may also include technical security controls and testing requirements for the cashless production environment.

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 and testing requirements, which will be assessed during evaluations of the cashless production 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.

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 Validation 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.

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 cashless 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 production 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.

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.

1.5 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. Unless otherwise directed by the regulatory body:

a) For unaltered commercial off-the-shelf (COTS) components, such as PCs or tablets, certification is not required; and
b) For modified off-the-shelf (MOTS) components, certification is required only to the modifications made to the components unless otherwise required by the regulatory body.

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 prior to and/or during implementation.

1.5.2 Operational Audits and Assessments

The integrity and accuracy of the operation of Cashless Systems and Technologies is highly dependent upon operational procedures, configurations, and the cashless 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 and assessments be conducted on a periodic basis:

a) An internal controls audit, against the applicable controls identified in the regulatory body's Minimum Internal Control Standards (MICS); and/or
b) A technical security assessment, against the applicable controls and tests identified in the GLI Gaming Security Framework (GLI-GSF), and/or any other controls and tests identified by the regulatory body.

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. The requirements of this chapter apply to Cashless Systems in addition to the applicable "General Gaming System Requirements" within the *GLI-13 Standards for Monitoring and Control Systems and Validation Systems* and/or other applicable technical requirements observed by the regulatory body.

2.2 Cashless System Communications

2.2.1 Cashless Device Monitoring

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

2.2.2 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 technical requirements observed by the regulatory body.

2.2.3 Cashless Transaction Communications

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

2.3 Cashless Information to be Maintained

2.3.1 Information Retention

The Cashless System shall be capable of maintaining and backing up all applicable recorded information as discussed within this standard in addition to the "Information to be Maintained" within the *GLI-13 Standards for Monitoring and Control Systems and Validation Systems* and/or other applicable technical requirements observed by the regulatory body, unless properly communicated to another Gaming System, which will assume these responsibilities.

NOTE: Internal controls may be in place to ensure this information is recorded where it is not maintained directly by the system.

2.3.2 Cashless Significant Event Information

In addition to the "System Significant Event Information" within the *GLI-13 Standards for Monitoring and Control Systems and Validation Systems* and/or other applicable technical requirements observed by the regulatory body, cashless significant event information to be maintained and backed up shall include, as applicable:

a) Large cashless transactions (single and aggregate over defined time period) in excess of a value specified by the regulatory body, including transaction information;
b) 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; and
   v. Negative account balance (due to adjustments and/or chargebacks).

2.3.3 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) The transaction value;
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).

NOTE: This information may be useful to monitor Cashless Device activity, including but not limited to, identifying cashless transactions without associated game play.

2.3.4 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) The date and method from which the account was opened (e.g., remote vs. on-site), including relevant location information;
c) For verified player accounts:
   i. The personally identifiable information (PII) collected by the operator to register a player and create the account, including, their full legal name, date of birth, residential address, contact information, and any other information required by the operator or the regulatory body;

ii. The player's full or partial government identification number (social security number, taxpayer identification number, passport number, or equivalent), and their current and previous personal financial information (credit or debit instrument 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. The date of player agreement to the operator's terms and conditions and privacy policies, including the versions agreed upon;
v. Previous accounts, if any, and reason for closure;

d) The account's current and previous authentication credentials, which shall be encrypted or hashed to a cryptographic algorithm as allowed by the regulatory body:
e) Account details and current balance. All discretionary account funds shall be maintained separately;
f) The date and time of account is accessed by any person (player or operator), including relevant location information;
g) Where supported, limitation/time-out/suspension information as required by the regulatory body:
   i. The date and time of the request;
   ii. Description and reason of limitation/time-out/suspension;
   iii. The type of limitation/time-out/suspension (e.g., system-imposed weekly deposit limitation, twenty-four-hour time-out, self-imposed monthly deposit limitation, self-imposed temporary suspension);
   iv. The date and time limitation/time-out/suspension commenced;
   v. The date and time limitation/time-out/suspension 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, credit or debit instrument, electronic payment account, etc.);
   x. Deposit authorization number;
   xi. Relevant location information.
i) The date and method from which the account was closed (e.g., remote vs. on-site), including relevant location information and reason for closure;
j) The current status of the player account (e.g., active, inactive, closed, suspended, etc.).

NOTE: This information may be useful to monitor player account activity, including but not limited to, identifying account openings and closings in short time frames and deposits and withdrawals without associated game play.

2.4 Cashless System Reports

2.4.1 General Statement

In addition to meeting the "General Reporting Requirements" within the *GLI-13 Standards for Monitoring and Control Systems and Validation Systems*, the Cashless System shall be capable of providing the necessary information to produce the reports listed in this section, unless properly communicated to another Gaming System, which will assume these responsibilities.

2.4.2 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.

2.4.3 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.

2.4.4 Cashier Summary and Detail Reports

The following information shall be provided to produce one or more reports for each cashier session at a Cashier Station which performs financial transactions for player accounts:

a) Unique Cashier Station ID or equivalent;
b) User account ID or name of cashier;
c) The date and time the cashier session began and ended;
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;
    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 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 electronically-based and 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 Reader

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 Reader

Barcode reader software shall be able to associate the barcode 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 Scanner

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 Device

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 (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 authentication 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 authentication 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 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 (e.g., transfer to/from Cashless Device, etc.);
b) The transaction value; and
c) For denied transactions, a descriptive message as to why the transaction did not complete as initiated.

3.4.3 Player Account Transfers

If the Cashless Device and the Cashless System support the ability to transfer funds between the player account and the Cashless Device for game play, the following shall apply:

a) After the player's identity is confirmed, funds may be transferred from their account balance to the Cashless Device's credit meter for game play. This may be automatic where the account balance is automatically transferred to the Cashless Device's credit meter or the player is presented transfer options, which require selection before occurring. Such options would include how much the player wishes to transfer to the Cashless Device's credit meter;
b) A transfer shall not be accepted that could cause the player to have a negative account balance. Where the account balance is less than the amount requested by the player, a transfer of the available funds may be processed provided that the player is clearly notified that they have transferred less than requested;
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 game play is completed, the player shall have the option to transfer some or all of their funds on the Cashless Device's credit meter back to their account balance or cash-out their funds via voucher issuance or another method. Funds may not be transferred from the Cashless Device to a different player account; and
e) Any funds on the Cashless Device that are attempted to be transferred to a player account on 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 another method), shall result in a handpay lockup or tilt on the Cashless Device.

3.4.4 Direct Account Wagering

If the Cashless Device and the Cashless System support the ability to directly wager from the player account balance (i.e., funds 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 account balance;
b) The account balance is to be debited when the wager is accepted by the Cashless System; and
c) The amounts won from game play shall automatically update the account balance or be available for further wagering or cash-out via voucher issuance or another method.

3.4.5 Electronic Funds Transfers

Where allowed by the regulatory body, cashless transactions may be performed using an electronic payment account. In the event of an electronic funds transfer to the Cashless Device, the Cashless System shall:

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

NOTE: The regulatory body may require electronic funds transfers to the Cashless Device to be performed in conjunction with a verified player account.

3.4.6 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.

3.4.7 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.

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 digits in length. Eight digits shall be used for the integer currency (e.g., dollar) amount and two 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:
   i. 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 or third-party financial services provider through a Cashless System or through the secure interface that uses a defined protocol;
   ii. 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;
   iii. 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;
   iv. 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 transactions that incremented any of the "Cashless Meters". The following information shall be displayed:

a) The type of transaction (e.g., transfer to/from Cashless Device, etc.);
b) The transaction value in local monetary units in numerical form;
c) The time of day of the transaction, in twenty-four 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 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.).

Chapter 4: Player Account Requirements

4.1 Introduction

4.1.1 General Statement

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

4.2 Verified Player Accounts

4.2.1 General Statement

The requirements of this section apply to registration, activation, and updates to verified player accounts where such functionality is supported directly by the Cashless System.

4.2.2 Player Account Registration

Prior to the establishment of a verified player account, there shall be a method to collect player's personally identifiable information (PII) for the registration process. During the registration process, the player shall:

a) Be denied the ability to register for a player account if they submit a birth date which indicates that they are underage;
b) If not all fields are required, 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;
c) Agree to the terms and conditions for accessing and using the player account and the privacy policies for PII protection;
d) Acknowledge that they are prohibited from allowing any unauthorized person to access or use their player account;
e) Consent to the monitoring and recording of the use of their player account by the operator and the regulatory body; and
f) Affirm that the PII the player is providing to open the player account is accurate.

NOTE: A player may hold only one active player account at a time unless specifically authorized by the regulatory body.

4.2.3 Identity Verification

Identity verification shall be undertaken before a verified player account is established. Third-party identity verification service providers may be used for identity verification.

a) Identity verification shall authenticate the player's full legal name, date of birth, and full or partial government identification number (driver's license number, social security number, taxpayer identification number, passport number, or equivalent) as required by the regulatory body.
b) 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.

c) Details of identity verification shall be kept in a secure manner.

NOTE: Additional identity verification checks may be conducted throughout the lifetime of the verified player account if the operator has reasonable suspicion that the player's identification has been compromised.

4.2.4 Account Activation

The verified player account can only be established 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 policies, and the player account registration is complete.

NOTE: When the terms and conditions and/or privacy policies are materially updated (i.e., beyond any grammatical or other minor changes), the player shall agree to their updates.

4.2.5 Account Updates

The player shall have the ability to access and update player account authentication credentials, registration information and the accounts used for financial transactions as supported by the system. Where supported, a multi-factor authentication process may be employed for account updates without gaming attendant involvement.

4.3 Unverified Player Accounts

4.3.1 General Statement

If supported by the Cashless System, unverified player accounts may be used where allowed by the regulatory body.

4.3.2 Account Balance Limits

If required by the regulatory body, the Cashless System shall enforce a maximum balance limit on the unverified 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.

4.4 Player Account Management

4.4.1 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) The player account shall be automatically locked-out after three successive failed active access attempts in a thirty-minute period, or a period to be determined by the regulatory body. Where supported, a multi-factor authentication process may be employed for a verified player account to be unlocked without attendant involvement. Alternatively, the system may, as supported, automatically release a locked-out account after thirty minutes, or a period to be determined by the regulatory body, has elapsed.
c) The system shall support a mechanism that allows for a player account to be locked-out or suspended in the event that other suspicious activity is detected. Where supported, a multi-factor authentication process may be employed for a verified player account to be unlocked without attendant involvement.
d) Where supported, a multi-factor authentication process may be employed for a player to retrieve or reset of their forgotten authentication credentials without gaming attendant involvement.

4.4.2 Financial Transactions

As supported, 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 locked-out 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 account may be unlocked; 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. Where supported, a multi-factor authentication process may be employed for a player to withdraw funds without gaming attendant involvement.

e) The system shall employ a mechanism that can detect and prevent any withdrawal activity initiated by a player that would result in a negative account balance. Where payment processing issues outside the control of the system cause an account to be overdrawn, the player account shall be suspended until the negative account balance is settled.
f) Payments from an account are to be paid (including funds transfer) directly to an account with a financial institution or third-party financial services provider in the name of the player or made payable to the player and forwarded to the player's residential address using a secure delivery service or through another method that is not prohibited by the regulatory body. For verified player accounts, the name and residential 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 account balances, and these changes are auditable.

4.4.3 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 financial and cashless 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) Funds added to/removed from the account balance from game play;
d) Manual adjustments or modifications to the account balance (e.g., due to refunds); and
e) Any other additions to, or deductions from, the account balance that would not otherwise be metered under any of the above-listed items.

NOTE: Where supported by the system, the player's self-imposed limitation, time-out, and suspension history may also be included.

4.4.4 Account Closure

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

4.5 Limitations, Time-Outs, and Suspensions

4.5.1 General Statement

The requirements in this section apply where the Cashless System supports the ability to directly manage and implement limitations, time-outs, and/or suspensions.

4.5.2 Limitations

Players shall be provided with a method to impose limitations for account activity including, but not limited to deposits and cashless transactions over a defined time period (e.g., day, week, month) as required by the regulatory body. In addition, there shall be a method for the system to impose any limitations for account activity 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 after the time period of the previous limit has expired, 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 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 time-outs or self-imposed suspension orders and revocations.

4.5.3 Time-Outs

Players shall be provided with a method to establish a time-out period up to seventy-two hours. In addition, there shall be a method for the operator to impose a time-out period on a player. During a timeout period, players may not conduct deposits and cashless transactions other than transferring funds from the Cashless Device back to their player account.

4.5.4 Suspensions

Players shall be provided with a method to suspend their player account for a specified period, which shall not be less than seventy-two hours, or indefinitely, as required by the regulatory body. In addition, there shall be a method for the operator to suspend a player account as required by the regulatory body. While a player account is suspended:

a) The player shall be given a notification that the account is suspended, the restrictions placed on the account, and general instructions for resolution where possible.
b) The player shall be prevented from:
    i. Performing cashless transactions other than transferring funds from the Cashless Device back to their player account;
    ii. Depositing funds with the exception of settling a negative account balance; and
    iii. Making changes to or closing their player account, unless authorized by the operator.
c) The player shall not be prevented from withdrawing any or all of their cashable player funds, provided that the operator acknowledges that the funds have cleared, and that the reasons for suspension would not prohibit a withdrawal.

Glossary of Key Terms

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 interleaved 2 of 5 barcodes, quick response (QR) codes, or any other machine-readable codes 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 ten 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 direct account wagering and 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 from their electronic payment account or a player account transfer. The term includes, without limitation, a prepaid access instrument.

Direct Account Wagering – Cashless transactions involving wagers placed directly from the player account balance, and amounts won from game play added directly to the player account balance, as supported.

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

EFT, *Electronic Funds Transfer* (aka "ECT", "Electronic Credits Transfer") – A financial transaction or cashless transaction involving an electronic transfer of funds between an electronic payment account and a player account or from an electronic payment account to a 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 third-party financial services provider, such as PayPal, Google Pay, or Apple Pay, for the purposes of making electronic funds transfers. The term does not include a player account, or any other account held by an operator and used 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.

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 full legal name, date of birth, place of birth, government identification number (driver's license number, social security number, taxpayer identification number, passport number, or equivalent), residential address, phone number, email address, personal financial information (credit or debit instrument numbers, bank account numbers, etc.), 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") –A cashless transaction where cashable player funds are electronically transferred between the Cashless Device and 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/Device – A card with embedded integrated circuits, or other technology, 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.

Unverified Player Account – A player account which has not gone through the age and identity verification process.

Verified Player Account – A player account which is registered to a player and has gone through the age and identity verification process.

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 gaming attendants and other 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.