STANDARDS FOR CASHLESS SYSTEMS

Table of Contents

COMMENTS

1) This draft revises GLI Standard 16 and is used with permission but GLI is not responsible for its contents. Most GLI markings have been removed to clarify that this document is a working document, at this time, of the CGA Regulatory Innovation Committee.
2) The revisions are intended to address or highlight the public policy issues that have been identified by the Regulatory Innovation Committee to date.
3) Some of the revisions may be better located in another document, i.e., internal controls or standard operating procedures for land-based gaming facilities operators. The intention is to have, at the very least, placeholders for discussion purposes.
4) Other GLI or equivalent standards related to integrity, security, privacy, etc. would continue to apply.

CHAPTER 1: INTRODUCTION TO CASHLESS SYSTEMS

1.1 Introduction

1.1.1 ***General Statement***. Cashless systems allow players to participate in wagering activities using an approved, securely protected authentication method, which accesses:

a) A player account at the cashless system of the operator; or
b) Another account of the player provided that it allows for the identification of the player and the source of funds and that is linked in a secure manner to the cashless system of the operator and the player account on that cashless system.

NOTE: *A cashless system may also support the functionality to communicate promotional awards to participating player accounts based upon predefined player activity criteria established by the parameters of the system. In this document, the term "cashless" shall be used to refer to both promotional and non-promotional functionality tied to a player account unless otherwise specified.*

1.1.2 ***Software Suppliers and Operators***. The components of a cashless system, although they may be constructed in a modular fashion, are designed to work seamlessly together. In addition, cashless systems may be developed to have configurable features; the final configuration of which depends on the options chosen by the operator. From a testing perspective, it might not be possible to test all of the configurable features of a cashless system 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. Because of the increasingly integrated nature of a cashless system, there are several requirements in this document which may apply to both operators and one or more suppliers. In such cases, the collection of solutions needed

to meet these requirements will be considered to be the cashless system and the individual entities providing them will need to meet such eligibility requirements as the provincial regulators deem appropriate for performance of these requirements.

1.2 Acknowledgment of Other Standards Reviewed

1.2.1 General Statement. This technical standard has been developed by reviewing and using portions of the **Gaming Laboratories International, LLC (GLI)** Technical Standard, *GLI-16 – Standards for Cashless Systems.*

1.3 Purpose of Standard

1.3.1 General Statement. The purpose of this technical standard is as follows:

a) To eliminate subjective criteria in analyzing and certifying cashless systems.
b) To only test those criteria which impact the credibility and integrity of gaming from both the revenue collection and player's perspective
c) To create a standard that will ensure that cashless operations are fair, secure, and able to be audited and operated correctly.
d) To distinguish between local public policy and Independent Test Laboratory criteria. It is up to each local jurisdiction to set its public policy with respect to gaming.
e) To recognize that non-gaming testing (such as electrical testing) should not be incorporated into this standard but left to appropriate test laboratories that specialize in that type of testing. Except where specifically identified in the standard, testing is not directed at health or safety matters. These matters are the responsibility of the manufacturer, purchaser, and operator of the equipment.
f) To recognize that the evaluation of internal control systems (such as anti-money laundering, financial and business processes) employed by the operators of the cashless system should not be incorporated into this standard but instead included within the regulatory operations of the province.

g) To construct a standard that can be easily revised to allow for new technology.

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

1.3.2 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. The document should not be interpreted that if the technology is not mentioned, then it is not allowed. To the contrary, as new technology is developed, this standard will be reviewed in order to make changes and incorporate new minimum standards for the new and related technology.

1.3.4 Adoption and Observance. This technical standard can be adopted in whole or in part by any provincial regulators that wish to implement a comprehensive set of requirements for cashless systems.

1.3.5 Scope of Standard. This technical standard will only govern cashless system requirements necessary to achieve certification when interfaced to kiosks, gaming devices, and/or any other equipment used for wagering at a gaming site, also known as cashless devices, for the purpose of communicating mandatory security events and electronic accounting meters, including with respect to any player's device or any other Approved Interface (OAI) such as an Application Programming Interface (API), Web API or similar software application on a player device (such as a smartphone or tablet) .

1.4 Other Documents That May Apply

1.4.1 Other Technical Standards. This technical standard covers the minimal requirements for Cashless Systems and all associated components. Depending on the technology utilized by a system, additional technical standards adopted by the provincial regulators may also apply.

1.4.2 Minimum Internal Control Standards (MICS). The implementation of a cashless system is a complex task, and as such will require the development of internal processes and procedures to ensure that the system is configured and operated with the necessary level of security and control. To that end, it is expected that the operator and/or provincial regulators will establish a set of Minimum Internal Control Specifications (MICS) to define the internal processes for the creation, 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.

1.4.3 Additional Standards. Where transactions from a financial institution or other approved source of funds are conducted, the operation of a cashless system shall be in or provide for compliance with the applicable portions of the "*Payment Card Industry Data Security Standard (PCI-DSS)*" and the "*Code of Conduct for the Credit and Debit Card Industry in Canada*".

1.5 Testing and Auditing

1.4.1 Laboratory Testing. The independent test laboratory will test and certify the components of the cashless system in accordance with the chapters of this technical standard within a controlled test environment, as applicable. Any of these requirements which necessitate additional operational procedures in place to meet the intent of the requirement shall be documented within the evaluation report and used to supplement the scope of the operational audit.

1.4.2 Operational Audit. The integrity and accuracy of the operation of a cashless system is highly dependent upon operational procedures, configurations, and the production environment's network infrastructure. In addition to the testing and certification of cashless system components, a provincial regulator may elect to require a periodic operational audit be conducted, using the recommended scope outlined within the appendix for "Operational Audit for Cashless Environments".

CHAPTER 2: CASHLESS DEVICE REQUIREMENTS

2.1 Introduction

2.1.1 ***General Statement***. The requirements throughout this chapter apply to kiosks, gaming devices and any other equipment used for wagering in the cashless environment, also known as cashless devices. These requirements are in addition to the requirements set forth in the provincial regulator's adopted requirements for kiosks, gaming devices, monitoring and control systems, and/or any other equipment used for wagering at a gaming site.

2.2 Device/API/OAI Requirements

2.2.1 ***Identifying a Cashless Device***. A player should be able to identify each cashless device by a means left to the discretion of the individual jurisdiction (e.g. remove display menu items that pertain to cashless operation for gaming devices or kiosks not participating; provide a host message indicating cashless capability; or a specific sticker on the gaming device or kiosk to indicate participation or non-participation).

2.2.2 ***Configuring Cashless Transactions***. Since a cashless feature 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.

2.2.3 ***Cashless Transaction Log***. Cashless devices shall have the ability to recall the last thirty-five (35) transactions that incremented any of the meters listed in the "Cashless Meter Requirements" section below. The following information must be displayed:

a) The type of transaction (upload/download) including restrictions (cashable, non-cashable, etc.);
b) The transaction value 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) The player account number or a unique transaction number, either of which can be used to authenticate the source of the funds (i.e. source of where funds came from/went to). If a player account number is displayed in the log, the cashless device shall mask all but the last four digits of the number.

NOTE: *It is also acceptable to have cashless transactions recorded in a larger log which also contains records of other types of transactions.*

2.2.4 ***Cashless Meter Requirements***. Cashless devices shall incorporate electronic accounting meters that shall conform to the following electronic metering requirements:

a) Cashless electronic accounting meters shall be at least ten (10) digits in length. Eight (8) digits shall be used for the dollar amount and two (2) digits used for the cents amount. The meter 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. The required electronic accounting meters are as follows:

   i. Electronic Funds Transfer In (EFT In). The cashless device must have a meter that accumulates the total value of cashable credits electronically transferred from a financial institution or other approved source of funds to the cashless device through a cashless system or through the API/OAI.

   ii. Player Account Transfer In (WAT In). The cashless device must have a meter that accumulates the total value of cashable credits electronically transferred to the cashless device from a player account by means of an external connection between the device and a cashless system or through the API/OAI .

   iii. Player Account Transfer Out (WAT Out). The cashless device must have a meter that accumulates the total value of cashable credits electronically transferred from

the cashless device to a player account by means of an external connection between the device and a cashless system or through the API/OAI.

iv. Cashable Electronic Promotion In (CEP In). The cashless device must have a meter that accumulates the total value of cashable promotional credits electronically transferred to the cashless device from a player account by means of an external connection between the device and a cashless system or through the API/OAI.

v. Cashable Electronic Promotion Out (CEP Out). The cashless device must have a meter that accumulates the total value of cashable promotional credits electronically transferred from the cashless device to a player account by means of an external connection between the device and a cashless system or through the API/OAI.

vi. Non-Cashable Electronic Promotion In (NCEP In). The cashless device must have a meter that accumulates the total value of non-cashable promotional credits electronically transferred to the cashless device from a player account by means of an external connection between the device and a cashless system or through the API/OAI.

vii. Non-Cashable Electronic Promotion Out (NCEP Out). The cashless device must have a meter that accumulates the total value of non-cashable promotional credits electronically transferred from the cashless device to a player account by means of an external connection between the device and a cashless system or through the API/OAI.

b) The operation of other mandatory electronic accounting 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.*

2.2.5 Diagnostic Tests on a Cashless Device. Controls must be in place for any diagnostic functionality available at the cashless device such that all activity must be reported to the 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.

2.2.6 ***Loss of Communication***. If communication between the cashless system and the cashless device is lost, a message must be displayed to the player that cashless transactions cannot currently be processed.

2.2.7 ***Protection of Sensitive Information***. The cashless device shall not allow any information contained in communication to or from the cashless system that is intended by the communication protocol to be protected, or which is of a sensitive nature, to be viewable through any display mechanism supported by the device. This includes, but is not limited to, validation numbers, secure PINs, player authentication credentials, or secure seeds and keys.

2.2 Player Identification Components

2.2.1 ***Player Identification Components.*** A player identification component is an electronic device 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 SMIB-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, biometric scanners, and wireless devices.

2.2.2 ***Card Readers.*** Card readers 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.

2.2.3 ***Barcode Readers.*** Barcode readers shall be able to associate the barcode visible on a card, wagering instrument, or an allowed software application on a player's wireless device, as applicable, with data stored in an external database as a means to identify an account association, or for the purpose of redemption.

2.2.4 Biometric Scanners. Biometric scanners 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 or for the purpose of redemption.

2.2.5 Wireless Devices. Communication between a cashless device and any wireless devices that are conducted using 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.*

2.2.6 Smart Card/Device Technology. If allowed by the provincial regulator, 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 is in agreement 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.*

2.2.7 ***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. A method for detection of counterfeiting shall be implemented;

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 non-integrated player identification component that holds information relating to cashless transactions in its memory shall not have means to compromise the information and shall not allow the removal of its information until that information has been successfully transferred and acknowledged by the cashless system.

2.2.8 ***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.

2.2.9 ***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 cashless system when such functionality is supported and possible.

CHAPTER 3: CASHLESS SYSTEM REQUIREMENTS

3.1 Introduction

3.1.1 ***General Statement***. A cashless system may be entirely integrated into an existing system, such as a monitoring and control system, or exist as an entirely separate entity. 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 chapter.

3.2 Control Program Requirements

3.2.1 ***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 provincial regulator. The critical control program authentication mechanism shall:

a) Employ a hash algorithm which produces a message digest of at least 128 bits;
b) Include all critical control program components which may affect player account operations, including but not limited to executables, libraries, wagering 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.

3.2.2 ***Control Program Independent Verification***. Each critical control program component of the cashless system shall have a method to be verified via for 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 and/or component approval, shall evaluate the integrity check method.

3.2.3 ***Shutdown and Recovery***. The cashless system shall be able to perform a graceful shut down, and only allow automatic restart on power up after the following procedures have been performed at a minimum:

a) Program resumption routine(s), including self-tests, complete successfully;
b) All critical control program components of the system have been authenticated using a method approved by the provincial regulator; and
c) Communication with all components necessary for system operation have been established and similarly authenticated.

3.3 Communication Requirements

3.3.1 ***Communications.*** The cashless system shall use communication techniques that have proper error detection and recovery mechanisms, which are designed to prevent intrusion, interference, eavesdropping and tampering. Any alternative implementations will be reviewed on a case-by-case basis.

3.3.2. ***Encryption.*** All data transmitted to and from the cashless device from the cashless system must employ a reasonable level of encryption for the information being transmitted. Additionally, the communication process used by the cashless device and the cashless system shall be:

a) Robust and stable enough to secure each cashless transaction such that failure event(s) can be identified and logged for subsequent audit and reconciliation; and
b) Protected against the capture of authentication data transmitted during the authentication and against manipulation by unauthorized parties.

3.3.3 ***Cashless Device Identification.*** The cashless system shall uniquely identify each cashless device connected to the system. This includes kiosks and any other equipment that are connected to the cashless system through a back-office platform or external system.

3.3.4 ***Monitoring*****.** The cashless system shall be equipped to read and store the applicable significant event and cashless transaction information, and specific cashless meter values from the cashless devices, as applicable to the system.

3.4 Information to be Maintained

3.4.1 ***Data Retention and Time Stamping***. The cashless system shall be capable of maintaining and backing up all recorded data as discussed within this section, unless properly communicated to a separate external system, who will address 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).

3.4.2 ***Player Account Information***. The information to be maintained and backed up shall include for each player account:

a) Unique player ID and player name;
b) Player data, including:
    i. All information collected by the operator to register a player and create the account;
    ii. 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;
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 (i.e. promotional credits that have a possible expiration) must be maintained separately;
e) Open text field for attendant input of player description or picture file (if applicable);
f) Previous accounts, if any, and reason for de-activation;
g) The date and method from which the account was registered (e.g., remote vs. on-site);
h) The date and time of last access;
i) Exclusions/limitations information, if supported by the system:

i. The date and time of the request (if applicable);
ii. Description and reason of exclusion/limitation;
iii. Type of exclusion/restriction (e.g., operator-imposed exclusion, self-imposed limitation);
iv. The date exclusion/limitation commenced;
v. The date exclusion/limitation ended (if applicable);

j) Financial transaction information:
i. Type of transaction (e.g., deposit, withdrawal, adjustment);
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 applicable);
vii. User identification or cashless device ID which handled the transaction (if applicable);
viii. Transaction status (pending, complete, etc.);
ix. Source of funds or method of deposit/withdrawal (e.g., cash, debit instruments, etc.);
x. Deposit authorization number; and
xi. Relevant location information.

3.4.3 <u>Promotion Information</u>. For cashless systems which support promotional awards that are redeemable for cash, wagering credits, or merchandise, the information to be maintained and backed up for each promotion offered shall include:

a) The date and time the promotional award period started and ended or will end (if known);
b) Current balance for promotional awards;
c) Total amount of promotional awards issued;
d) Total amount of promotional awards redeemed;
e) Total amount of promotional awards expired;
f) Total amount of promotional award adjustments; and

g) Unique ID for the promotional award.

3.4.4 Significant Event Information. Significant event information to be maintained and backed up shall include:

a) Failed login attempts;
b) Program error or authentication mismatch;
c) Significant periods of unavailability of any critical component of the system;
d) System voids, overrides, and corrections;
e) Changes to promotional parameters, if supported by the system;
f) Adjustments to a player account balance;
g) Changes made to player data and sensitive information recorded in a player account;
h) Deactivation of a player account;
i) Large financial transactions (single and aggregate over defined time period) in excess of a value specified by the provincial regulator, if supported by the system;
j) Large wins (single and aggregate over defined time period) in excess of a value specified by the provincial regulator, if supported by the system;
k) Large wagers (single and aggregate over defined time period) in excess of a value specified by the provincial regulator, if supported by the system;
l) Irrecoverable loss of sensitive information;
m) Any other activity requiring user intervention and occurring outside of the normal scope of system operation; and
n) Other significant or unusual events as deemed applicable by the provincial regulator.

3.5 Reporting Requirements

3.5.1 General Reporting Requirements. The cashless system shall be capable of generating the information needed to compile reports as required by the provincial regulator, unless properly communicated to a separate external system, who will address 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) The system shall be able to provide the reporting information on demand and for intervals required by the provincial regulator including, but not limited to, daily, month-to-date (MTD), year-to-date (YTD), and life-to-date (LTD).

b) Each required report shall contain:

   i. The gaming site and/or operator, the selected interval and the date/time the report was generated; and

   ii. An indication of "No Activity" or similar message if no information appears for the period specified.

3.5.2 <u>Financial and Player Reports</u>. The cashless system shall be able to provide the information needed to provide the following financial and player reports, unless properly communicated to a separate external system, who will address these responsibilities:

a) <u>Cashless System Activity Reports</u>. These reports are to include deposits, transfers to and from cashless devices, withdrawals, adjustments and balances, by player account.

b) <u>Liability Reports</u>. These reports are to include previous days ending value (today's starting value) of outstanding cashless liability, total cashless-in and total cashless out, expired promotional value (where supported), and the current day's ending cashless liability, if applicable. Separate reports may be generated for promotional and non-promotional cashless liability.

c) <u>Cashless Meter Reconciliation Summary and Detail Reports</u>. These reports will reconcile each cashless device's cashless meter(s) against the system's cashless activity. Separate reports may be generated for promotional and non-promotional cashless activity.

d) <u>Cashier Summary and Detail Reports</u>. To include player account, deposits and withdrawals, amount of transaction, date and time of transaction. player account, and cashier starting and ending balances, session start and end date/time (etc.) by cashier.

e) <u>Significant Event Report</u>. One or more reports for each significant event or alteration as applicable which shall include:

   i. The date and time of the significant event or alteration;

   ii. Event/component identification (if applicable);

iii. Identification of user(s) who performed and/or authorized the significant event or alteration;

iv. Reason/description of the significant event or alteration, including data or parameter altered;

v. Data or parameter value before alteration; and

vi. Data or parameter value after alteration.

CHAPTER 4: PLAYER ACCOUNT REQUIREMENTS

4.1 Introduction

4.1.1 ***Introduction***. The following chapter applies to player accounts and cashless transactions in addition to the "Player Account Controls" section within this document.

4.2 Player Account Access and Maintenance

4.2.1 ***Player Authentication***. All cashless transactions between a supporting cashless device and the cashless system must be secured using a method of authentication, such as debit instrument or card insertion or "tap" (contactless) capacity on the player identification component and PIN entry, a similar approved process that allows for the identification of the player and the source of funds if a software application on a player's device is used, or a secure alternative means (e.g. finger-print recognition). Authentication methods are subject to the discretion of the provincial regulator 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.

a) If the system does not recognize the authentication credentials provided by the player, an explanatory message shall be displayed to the player which prompts the player to try again.
b) Where a player has forgotten their authentication credentials, a multi-factor authentication process shall be employed for the retrieval of their authentication credentials.
c) Current account balance information and transaction options shall be available to the player once authenticated.
d) The system shall support a mechanism that allows for an account to be locked in the event that suspicious activity is detected. A multi-factor authentication process shall be employed for the account to be unlocked.
e) Player accounts are automatically locked-out after three failed access attempts in a thirty-minute period. The system may release a locked-out account after thirty minutes has elapsed. If a gaming site employee 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 employee assisting in unlocking the account), the elapsed time of thirty minutes is not required.

4.2.2 Modification of Player Information. The system shall allow the ability to 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.

4.2.3 Maximum Balance Limits. Where supported by the system and required by the provincial regulator, the system must enforce a maximum balance limit on the player account.

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

4.2.4 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 details on the following types of cashless transactions (time stamped with a unique transaction ID):

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) Promotional awards credits added to/removed from the player account;
e) Manual adjustments or modifications to the player account (e.g., due to refunds); and
f) Any other additions to, or deductions from, the player account, that would not otherwise be metered under any of the above listed items.

4.3 Cashless Transactions

4.3.1 ***Transaction Identifier***. For all cashless transactions initiated at a cashless device, cashless systems shall assign to each transaction a unique identifier of at least eight digits that includes the cashless device designation.

4.3.2 ***Prohibition of Credit Card Use***. Unless otherwise allowed by the provincial regulator, cashless systems shall prevent the direct wagering at a cashless device or an electronic funds transfer to a cashless device or player account through the use of a credit card.

4.3.3 ***Financial Transactions***. Funds may be deposited to or withdrawn from the player account via a cashier or any supporting cashless device (through coins/tokens, bills, wagering instruments, debit instruments, etc.) or from an approved Application Programming Interface (API), Web API or similar software application on a player's device (such as a smartphone or tablet) that complies with the requirements with respect to player identification and source of funds. Cashless transactions are entirely electronic.

a) Funds may also be added from an approved third-party API/OAI, or similar software application on a player's device (such as a smartphone or tablet) that complies with the requirements with respect to player identification and source of funds.

b) Where allowed by the provincial regulator, a deposit into a player account may be made via a debit instrument transaction which can produce a sufficient audit trail. These funds shall not be available for wagering until:
   i. The funds are received from the issuer; or
   ii. The issuer provides an authorization number indicating that the funds are authorized. The authorization number is to be maintained in an audit log

c) Cashless systems shall, in the event of a debit instrument transaction:
   i. Provide for on-line, real-time validation of debit instruments, as applicable;
   ii. Execute the transaction in accordance with all applicable provincial and federal electronic funds transfer requirements or player account transfer requirements including receipting and fee disclosure requirements;
   iii. Not execute a transaction upon notification from the player's financial institution

that the available funds in the player's account associated with the player's debit instrument are less that the amount requested by the player; and

iv. Provide notice to the player that funds may be approved for transfer from sources other than the account associated with the player's debit instrument, as determined by the player's financial institution.

d) Where the player initiates a contactless electronic payment transaction, the following conditions shall be met:

i. The individual amount of the contactless electronic payment transaction limit shall be configurable as required by the provincial regulator;

ii. The cumulative amount of previous contactless electronic payment transactions limit shall be configurable as required by the provincial regulator;

iii. The number of consecutive contactless electronic payment transactions initiated since multi-factor authentication shall not exceed five; and

iv. The maximum time without activity by the player after being authenticated for accessing their payment account shall not exceed five minutes.

e) Cashless devices that permit players to withdrawal funds without interacting with the operator must authenticate users using multi-factor authentication.

f) It shall not be possible to transfer funds directly between two player accounts.

4.3.4 ***<u>Game Play Transactions</u>***. Depending on what is supported by the system and the cashless device, the cashless device may present transfer options to the player, which require selection before occurring.

a) Where credits are transferred between the player account and to the cashless device:

i. Players may have the option of moving some or all of their system credit to the cashless device they are playing through "withdrawal" from the player account. Some systems may move either a predefined amount or the player's entire balance to the cashless device for play; and

ii. A transfer shall not be accepted that could cause the player to have a negative balance; and

iii. The account balance is to be debited when the transfer is accepted by the system.

iv. When they are finished playing, the player may have the option to "deposit" their credit balance from the cashless device onto their player account or cash out some credits. Some systems may require that the entire currency value of the credit balance be transferred back to the system.

v. 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 hopper or printer), must result in a hand-pay lockup or tilt on the cashless device.

b) Where credits are not transferred between the player account and to the cashless device (i.e. direct wagering from the player account is occurring):

i. A wager shall not be accepted that could cause the player to have a negative balance; and

ii. The account balance is to be debited when the wager is accepted by the system.

c) If non-cashable credits and cashable player funds are comingled on one credit meter, non-cashable credits shall be wagered first, as allowed by the rules of the game, before any cashable player funds are wagered.

4.3.5 ***Transaction Messages***. Cashless systems shall cause a relevant, informative message to be displayed to the player whenever any cashless transaction is being processed. The cashless device, player identification component display, or the player's device with an API/OAI must be capable of providing confirmation/denial of every cashless transaction initiated. This confirmation/denial must include:

a) The type of transaction (upload/download);

b) The transaction value;

c) For denied transactions, a descriptive message as to why the transaction did not complete as initiated.

4.3.6 ***Transfer of Transactions***. If a player initiates a cashless transaction and that transaction would exceed cashless devices configured limits (i.e. the credit limit, transaction limit, etc.) or any limit that has been established for purposes of responsible gambling then this transaction may only

be processed provided that the player is clearly notified that he has received or deposited less than requested to avoid player disputes.

4.3.7 ***Limitations and Exclusions.*** Where supported by the system, the cashless system shall be able to correctly implement any limitations and/or exclusions put in place by the player and/or operator as required by the provincial regulator. Where the system provides the ability to directly manage limitations and/or exclusions, the applicable requirements within the "Limitations" and "Exclusions" sections of this document shall be evaluated.

4.4 Access to Player Account Remotely

4.4.1 ***General Statement.*** Depending on the implementation(s) authorized by the provincial regulator, a player may be allowed to access their player account and/or perform financial transactions remotely directly using approved API/OAI or similar application or software package on a player's device. Examples of a player's device include a personal computer, mobile phone, tablet, etc. In addition to the previous section, the requirements of this section shall be met.

NOTE: *Nothing in this section should be interpreted as being applicable to wagering using a player's device.*

4.4.2 ***Software Identification.*** The software shall contain sufficient information to identify the software and its version.

4.4.3 ***Device-System Interactions.*** The player may obtain/download an application or software package or access the software via a browser to access their player account on the cashless system.

a) Players shall not be able to use the software to transfer data to one another, other than chat functions (e.g., text, voice, video, etc.) and approved files (e.g., user profile pictures, photos, etc.);
b) The software shall not automatically alter any device-specified firewall rules to open ports that are blocked by either a hardware or software firewall;

c) The software shall not access any ports (either automatically or by prompting the user to manually access) which are not necessary for the communication between the player's device and the system;

d) If the software includes additional non-account related functionality, this additional functionality shall not alter the software's integrity in any way;

e) The software shall not possess the ability to override the volume settings of the device;

f) It is recommended that auto complete, password caching, or other methods that will fill in the password field are disabled by default for the software.

4.4.4 Compatibility Verification. During any installation or initialization and prior to commencing player account access, the software used in conjunction with the cashless system shall detect any incompatibilities or resource limitations with the player's device that would prevent proper operation of the software (e.g., software version, minimum specifications not met, browser type, browser version, plug-in version, etc.). If any incompatibilities or resource limitations are detected the software shall prevent player account access and display an appropriate error message.

4.4.5 Software Content. The software shall not contain any malicious code or functionality deemed to be malicious in nature by the provincial regulator. This includes, but is not limited to, unauthorized file extraction/transfers, unauthorized device modifications, unauthorized access to any locally stored personal information (e.g., contacts, calendar, etc.) and malware.

4.4.6 Cookies. Where cookies are used, players shall be informed of the cookie use upon software installation or during player registration. When cookies are required for access, access cannot occur if they are not accepted by the player's device. All cookies used shall contain no malicious code.

4.4.7 Information Access. The items specified in the "Information for Player Accounts" section of this document shall be displayed, either directly from the player's device screen or from a page accessible to the player.

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

b) The display of this information shall be adapted to the player's device. For example, where a player's device uses technologies with a smaller display screen, it is permissible to present an abridged version of the this information accessible directly from within the player's device screen and make available the full/complete version of the information via another method, such as a secondary screen, help menu, or other interface that is easily identified on the visual screen.

4.4.8 Player Access. A player accesses their player account remotely using a username (or similar) and a password or a secure alternative means for the player to perform authentication to log in to the cashless system. After 30 minutes of inactivity on a player's device, or a period determined by the provincial regulator, the player shall be required to re-authenticate to access their player account. A simpler means may be offered for a player to re-authenticate on that device, such as operating system-level authentication (e.g., biometrics) or a PIN. Each means for re-authentication will be evaluated on a case-by-case basis by the independent test laboratory.

a) This functionality may be disabled based on preference of the player and/or provincial regulator.

b) Once every 30 days, or a period specified by the provincial regulator, the player will be required to provide full authentication on that device.

4.5 Player Loyalty Programs

4.5.1 Player Loyalty Programs. Player loyalty programs are any programs that provide promotional awards for players, typically based on the volume of play or revenue received from a player. If player loyalty programs are supported by the cashless system, the following principles shall apply:

a) All awards shall be equally available to all players who achieve the defined level of qualification for player loyalty points;

b) Redemption of player loyalty points earned shall be a secure transaction that automatically debits the points balance for the value of the points redeemed; and

c) All player loyalty points transactions shall be recorded by the system.

APPENDIX A: OPERATIONAL AUDIT FOR CASHLESS ENVIRONMENTS

A.1 Introduction

A.1.1 ***General Statement***. This appendix sets forth recommended technical security controls, procedures and practices for cashless environments which, if required by a provincial regulator, will be reviewed in an periodic operational audit, including, but not limited to, player account management, review of the operational processes that are critical to compliance, storing and/or processing player data, handling various financial transactions, fundamental practices relevant to the limitation of risks, and any other objectives established by the provincial regulator.

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

A.2 General Operating Procedures

A.2.1 ***Internal Control Procedures.*** The operator shall establish, maintain, implement and comply with internal control procedures for player account operations, including performing financial transactions. 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) Employee 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 provincial regulator.

A.2.2 Operator Reserves. The operator shall have processes in place for maintaining and protecting adequate cash reserves, as determined by the provincial regulator, including segregated accounts of funds held for player accounts and operational funds.

A.2.3 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 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 wagering 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.2.4 Anti-Money Laundering (AML) Monitoring. The operator shall have AML procedures and policies put in place, as required by the provincial regulator, to ensure:

a) Employees are trained in AML, and this training is kept up to date;
b) Cashless devices are monitored for funds transferred into the cashless device from one player account then transferred out to another player account;
c) Player accounts are monitored for opening and closing in short time frames and for deposits and withdrawals without associated game play transactions;

d) Aggregate transactions for a player account over a defined period may require further due diligence checks and may be reportable to the relevant organization if they exceed the threshold prescribed by the provincial regulator;

e) Identification of a player and the player's source of funds for purposes of anti-money laundering requirements under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, including any risk assessments or reporting requirements pursuant to *PC(ML)TFA*, its regulations and guidance from the Financial Transactions and Reports Analysis Centre, and any requirements observed by provincial regulators, in order to trigger an appropriate response by the operator; and

f) Unless authorized by the provincial regulator, the cashless operation does not permit the use of virtual currency as defined by the regulations under *PC(ML)TFA*, cryptocurrencies or other currencies which are dependent upon any other factor to determine value, other than any relevant currency exchange with respect to the Canadian dollar.

A.3 Player Account Controls

A.3.1 ***Registration and Verification.*** There shall be a method to collect player data prior to the registration of a player account. Where player account registration and verification are supported by the cashless system either directly by the system or in conjunction with a third-party service provider's software, the following requirements shall be met:

a) Only players of the legal wagering age for the jurisdiction may register for a player account. Any person that submits a birth date that indicates they are underage shall be denied the ability to register for a player account.

b) During the registration process, the player shall agree to the terms and conditions and privacy policy and affirm that:

   i. The information provided by the player to the operator to open the player account is accurate;

   ii. The player has been informed of and acknowledged that they are prohibited from allowing any other person not assigned to the player account access to or use of their player account; and

iii. The player consents to the monitoring and recording by the operator and the provincial regulator of the use of their player account.

c) Identity verification shall be undertaken before a player is allowed to place a wager. Third-party service providers may be used for identity verification as allowed by the provincial regulator.

i. Identity verification shall authenticate the legal name, physical address and age of the individual at a minimum as required by the provincial regulator.

ii. Identity verification shall also confirm that the player is not on any exclusion lists held by the operator or the provincial regulator or prohibited from establishing or maintaining an account for any other reason.

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

d) 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 privacy policies and terms and conditions, and the player account registration is complete.

e) A player shall only be permitted to have one active player account at a time unless specifically authorized by the provincial regulator. There shall be an established procedure for the authorized use of multiple player accounts.

NOTE: *An operator may assign more than one player to a single player account provided that each additional player is registered as provided herein.*

A.3.2 <u>Fraudulent Accounts</u>. 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.3.3 ***<u>Player Data Security</u>.*** Any information obtained in respect to the player account, including player data and authentication credentials, shall be done in compliance with the privacy policy and local privacy regulations and standards observed by the provincial regulator. Both player data and the player funds shall be considered as critical assets for the purposes of risk assessment. In addition:

a) Any player data 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 or cashless device;
   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 provincial regulator or the operator.

b) There shall be procedures in place for the security and sharing of player data, funds in a player account and other sensitive information as required by the provincial regulator, including, but not limited to:
   i. The designation and identification of one or more employees 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 provincial regulator.

A.3.4 <u>Financial Transactions</u>. Procedures shall be in place to ensure all financial transactions are conducted in accordance with local commerce regulations and requirements mandated by the provincial regulator:

a) Where such 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 procedure shall be established specifying thresholds of payment and methods of withdrawal.

c) The operator shall neither extend credit to a player nor allow the deposit of funds into a player account that are derived from the extension of credit by affiliates or agents of the operator. For purposes of this subsection, credit shall not be deemed to have been extended where, although funds have been deposited into a player account, the operator is awaiting actual receipt of such funds in the ordinary course of business.

d) The operator shall not allow a player account to be overdrawn unless caused by payment processing issues outside the control of the operator.

e) For withdrawals not paid directly to the player, 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.

f) 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 provincial regulator.

g) The operator shall have security or authorization procedures in place to ensure that only authorized adjustments can be made to player accounts, and these changes are auditable.

h) All financial transactions shall be reconciled with financial institutions and payment processors daily or as otherwise specified by the provincial regulator.

A.3.5 ***Securing Payment Methods.*** To protect payments methods against fraudulent uses, the following controls shall apply:

a) Collection of sensitive information directly related to financial transactions shall be limited to only the information strictly needed for transaction.
b) Adequate measures shall be taken in order to protect any type of payment used in the system from a fraudulent use.
c) The operator shall verify that the payment processors ensure the protection of the player data, including any sensitive information given by the player or transaction related data.
d) There shall be an established procedure for assuring the match of ownership between the payment type holder and the player account holder.
e) The operator shall generate all transactional records of player accounts. The data recorded shall allow the operator to trace a single financial transaction of a player from another transaction.

A.3.6 ***Limitations.*** If supported in the cashless environment, players shall be provided with a method to impose limitations for gaming parameters including, but not limited to deposits and wagers as required by the provincial regulator. If supported, there shall also be a method for the operator to impose any limitations for gaming parameters as required by the provincial regulator.

a) Once established by a player and implemented by the operator, it shall only be possible to reduce the severity of self-imposed limitations upon 24 hours' notice, or as required by the provincial regulator;
b) Players shall be notified in advance of any operator-imposed limits and their effective dates. Once updated, operator-imposed limits shall be consistent with what is disclosed to the player;
c) Upon receiving any self-imposed or operator-imposed limitation order, the operator 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; and

d) The self-imposed limitations set by a player shall not override more restrictive operator-imposed limitations. The more restrictive limitations shall take priority; and

e) Limitations shall not be compromised by internal status events, such as self-imposed exclusion orders and revocations.

A.3.7 ***Exclusions***. If supported in the cashless environment, players shall be provided with a method to exclude themselves from gaming for a specified period or indefinitely, as required by the provincial regulator. If supported, there shall also be a method for the operator to exclude a player from gaming as required by the provincial regulator.

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 withdraw; and

d) All advertising or marketing material shall not specifically target players that have been excluded from play.

A.3.8 ***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) Allow access by player to their inactive account only after performing additional identity verification;

b) Protect inactive accounts that contain funds from unauthorized access, changes or removal; and

c) Deal with unclaimed funds from inactive accounts, including returning any remaining funds to the player where possible.

A.3.9 ***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.

A.3.10 ***Internal Audits***. Internal audits must be performed by operator personnel independent of the transactions being audited. Supervision must be provided as needed for internal auditing by personnel with authority equal to or greater than those being supervised.

a) Controls must be established, and procedures must be implemented to perform the following procedures:
   i. At least weekly, reconcile player account liability (deposits ± adjustments−withdrawals = total account balance) to the system record.
   ii. At least weekly, review manual adjustments to/from player accounts to ensure such adjustments were authorized;
   iii. At least monthly, review exception reports;
   iv. At least monthly, review documentation related to access to inactive and closed accounts; and
   v. At least annually, review the cashless system to determine that the configuration parameters are accurate and have not been altered without appropriate authorization.

b) The performance of internal audit procedures, the exceptions noted, and the follow-up of all internal audit exceptions must be documented and maintained.

A.4 Information for Player Accounts

A.4.1 ***General Statement.*** The following requirements apply to information displays for a player account, and/or information regarding a player account that is otherwise provided to players via external signage, forms, or brochures available at the gaming site.

A.4.2 ***Terms and Conditions.*** A set of terms and conditions shall be available to the player. The

terms and conditions shall:

a) Advise the player to keep their authentication credentials secure;
b) Disclose all processes for dealing with lost authentication credentials, forced changes, and other related items;
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) Disclose the operator's policy regarding the acceptance of debit instruments, and electronic funds transfer to the player;
e) 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 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.4.3 ***Privacy Policy.*** A privacy policy shall be available to the player. The privacy policy shall state:

a) The player data required to be collected;
b) The purpose for information collection;
c) The period in which the information is stored;
d) The conditions under which information may be disclosed; and
e) An affirmation that measures are in place to prevent the unauthorized or unnecessary disclosure of the information.

A.4.4 ***Player Protection Information.*** Player protection information shall be available to the player. The player protection information shall contain at a minimum:

a) Information about potential risks associated with excessive gambling, and where to get

help for a gambling problem;

b) A list of the available player protection measures that can be invoked by the player, such as self-imposed exclusion, and information on how to invoke those measures;

c) Mechanisms in place which can be used to detect unauthorized use of their account, such as reviewing debit card statements against known deposits;

d) Contact information or other means for reporting a complaint/dispute; and

e) Contact information for the provincial regulator and/or a link to their website.

A.4.5 Promotional Awards. If supported in the cashless environment, players shall be able to access information pertaining to any available promotional awards, including how the player is notified when they have received a promotional award and the terms of their withdrawal. This information shall be clear and unambiguous, especially where promotional awards are limited to certain games, paytables, or when other specific conditions apply.

A.5 Technical Security Controls

A.5.1 Physical Location of Components. The cashless system components shall be housed in a secure environment which shall:

a) Have sufficient protection against alteration, tampering or unauthorized access; and

b) Be equipped with a surveillance system that shall meet the procedures put in place by the provincial regulator.

A.5.2 Logical Access Control. The cashless environment shall be logically secured against unauthorized access by authentication credentials allowed by the provincial regulator, such as passwords, multi-factor authentication, digital certificates, PINs, biometrics, and other access methods (e.g., magnetic swipe, proximity cards, embedded chip cards). The number of users that have the requisite permissions to adjust critical parameters shall be limited.

A.5.3 ***Prevention of Unauthorized Transactions***. The following minimal controls shall be implemented by the cashless system to ensure that cashless devices are prevented from responding to commands for crediting outside of properly authorized cashless transactions (hacking):

a) All network hubs, services and connection ports shall be secured to prevent unauthorized access to the network;
b) The number of workstations where critical cashless applications or associated databases may be accessed shall be limited; and
c) Procedures shall be in place to identify and flag suspect player and employee accounts to prevent their unauthorized use to include:
    i. Having a maximum number of three incorrect attempts at authentication before account lockout;
    ii. Flagging of suspect accounts where authentication credentials may have been stolen;
    iii. Invalidating accounts and transferring balances into a new account; and
    iv. Establishing limits for maximum cashless activity or overall wagering activities in and out as a global or individual variable to preclude money laundering.

A.5.4 ***Encryption Method.*** The cashless environment shall utilize an encryption method which includes the use of different encryption keys so that encryption algorithms can be changed or replaced as soon as practical. Other methodologies shall be reviewed on a case-by-case basis.

A.5.5 ***Data Alteration.*** The alteration of any accounting, reporting or player data shall not be permitted without supervised access controls. In the event any data is changed, the following information shall be documented or logged:

a) Unique ID number for the alteration;
b) Data element altered;
c) Data element value prior to alteration;
d) Data element value after alteration;
e) Time and date of alteration; and

f) Personnel that performed alteration (user identification).

A.5.6 ***Generation and Storage of Logs.*** Logs shall be generated on each system component where supported in order to monitor and rectify anomalies, flaws and alerts.

A.5.7 ***Storage Medium Backup.*** Audit logs, system databases, and any other pertinent sensitive data specified in the under the section entitled "Information to be Maintained" shall be stored using reasonable protection methods for a period of five years or as otherwise specified by the provincial regulator. The cashless environment shall be designed to protect the integrity of this data in the event of a failure. Redundant copies of this data shall be kept on the cashless system with open support for backups and restoration, so that no single failure of any portion of the system would cause the loss or corruption of data.

A.5.8 ***Uninterruptible Power Supply (UPS) Support.*** All components in the cashless environment shall be provided with adequate primary power. Where the cashless system is a stand-alone application, it shall have an Uninterruptible Power Supply (UPS) connected and shall have sufficient capacity to permit a graceful shut-down and that retains all pertinent sensitive information during a power loss. It is acceptable that the system may be a component of a network that is supported by a network-wide UPS provided that the system is included as a component protected by the UPS. There shall be a surge protection system in use if not incorporated into the UPS itself.

A.5.9 ***Security Testing.*** The operator shall provide a layered approach to security within the cashless environment to ensure secure storage and processing of data. In addition, as required by the provincial regulator:

a) All entry and exit points to open public network systems shall be identified, managed, monitored and controlled.
b) The operator shall monitor all its cashless systems in order to prevent, detect, mitigate and respond to cyberattacks.

c) Appropriate measures shall be in place to detect, prevent, mitigate and respond to common active and passive technical attacks.

d) The operator shall have an established procedure to gather cyber threat intelligence and act on it appropriately.

e) Technical security tests on the cashless environment, including vulnerability assessments and penetration testing, shall be performed annually as required by the provincial regulator to guarantee that no vulnerabilities putting at risk the security and operation of the cashless system exist.

f) There shall be appropriate security testing on major cashless system changes. The operator shall also have agreed patching policies for cashless systems, whether developed and supported by the operator or by a third-party service provider.

GLOSSARY OF KEY TERMS

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

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.

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

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

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

Barcode – An optical machine-readable representation of data. A good example is a barcode found on printed wagering instruments.

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.

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

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

Cashable Player Funds – Cashable Credits and Cashable Promotional Credits that are redeemable for cash.

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

Cashless Device – An electronic device that converts communications from the cashless system into a human interpretable form and converts human decisions into communication format

understood by the cashless system. Cashless devices refer to kiosks, gaming devices and any other equipment used for wagering at a gaming site.

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 another account of the player provided that it allows for the identification of the player and the source of funds and that is linked in a secure manner to the cashless system of the operator and the player account on that cashless system. The system provides the operator with the means to review player accounts, generate various cashless transaction and account reports, and set any configurable parameters. A cashless system may also support the functionality to communicate promotional awards to participating player accounts based upon predefined player activity criteria established by the parameters of the system.

Cashless Transactions – The electronic transfer to or from a cashless device of a player's credits, through the use of a cashless system. The term also includes electronic funds transferred from a financial institution to a cashless device as a result of an electronic funds transfer through a cashless system.

CEP, *Cashable Electronic Promotion* – Cashable promotional credits electronically transferred to/from a cashless device from/to a player account.

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

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.

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.

EFT, *Electronic Funds Transfer* (aka "ECT", "Electronic Credits Transfer") – An electronic transfer of funds from an independent financial institution to a cashless device through a cashless system.

Electronic Accounting Meter (aka "Software Meter" / "Soft Meter") – An accounting meter that is implemented in the main program software of a cashless device.

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

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

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

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.

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

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 system.

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).

NCEP, *Non-Cashable Electronic Promotion* – Non-cashable promotional credits electronically transferred to/from a cashless device from/to a player account.

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

Operator – A person or entity that operates a cashless system, using both the technological capabilities of the cashless system as well as their own internal procedures.

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

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

PIN, *Personal Identification Number* – 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 for a player where information relative to financial and wagering 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 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") – An electronic transfer of funds between a cashless system's player account and a gaming device.

Player Data – Sensitive information regarding a player and which may include items such as full name, date of birth, place of birth, social security number, address, phone number, medical or employment history, or other personal information as defined by the regulatory body.

Player Identification Component – A player identification component is an electronic device 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.

Player Loyalty Program – A program that provides promotional awards for players based on the volume of play or revenue received from a player.

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.

Printer – A peripheral that prints wagering instruments and other items as necessary.

Promotional Award – An award that is not described in the paytable of a game, that is based upon predefined player activity criteria established by the parameters of the cashless system that are tied to a specific player account, which generally recur. Examples include earning non-cashable credits which match their first deposit, awarding points for a certain amount of credits played on a game; awarding credits for wagering more than a certain amount of credits within a specific time period.

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

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

SMIB, Slot Machine Interface Board – A circuit board that interfaces the cashless device with an external system, supporting protocol conversion between the machine and the system.

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.

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

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