BERMUDA GAMING COMMISSION (BGC)

BGC-4 CASINO GAMING CASHLESS WAGERING SYSTEM STANDARDS

VERSION: 1.1

RELEASE DATE: OCTOBER 22, 2021

Table of Contents

CHAPTER 1: INTRODUCTION

1.1 Introduction

1.1.1 General Statement.

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

The criteria are not exhaustive. All statutory requirements contained in the Gaming Act 2014 ("the Act") and the Gaming (Casino) Regulations 2018 ("the Regulations") shall be observed. This standard expressly applies for the purposes of the Regulations and section 93 of the Act.

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

1.2 Purpose of Equipment Standards

1.2.1 Purpose.

The purpose of this equipment standard is as follows:

a) To eliminate subjective criteria in analyzing and certifying Cashless Wagering Systems;

b) To primarily test those criteria which impact the credibility and integrity of gaming from both the revenue collection and patron'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 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;

e) To recognize that the evaluation of internal control systems (such as anti-money laundering/anti-terrorist financing, financial and business processes) employed by the operators of the Cashless Wagering System should not be incorporated into this standard but instead included within the operational audit performed;

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

g) 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.

1.2.2 No Limitation of Technology.

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

1.3 Interpretation of this Document

1.3.1 General Statement.

A Cashless Wagering System uses a method of wagering and accounting in which:

a) The validity and value of a wagering instrument or wagering credits are determined, monitored and retained by a computer operated and maintained by an operator which maintains a record of each transaction involving the wagering instrument or wagering credits, exclusive of any event, game or cashless terminal on which wagers or bets are being made;

b) Patrons are able to participate in gaming activities using an approved, securely protected authentication method, which accesses:

   i. A patron account at the Cashless Wagering System of the operator; or

   ii. Another account of the patron provided that it allows for the identification of the patron and the source of funds and that is linked in a secure manner to the Cashless Wagering System of the operator and the patron account on that Cashless Wagering System.

c) Computerised or electronic monitoring systems facilitate electronic transfers of money directly to or from a game or cashless terminal.

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

1.3.2 Scope of Standard.

This technical standard will only govern Cashless Wagering System and Patron Account requirements necessary to achieve certification when interfaced to gaming machines,

kiosks (including betting terminals), and/or any other equipment used for physical gaming at a gaming premises, also known as cashless terminals, for the purpose of communicating mandatory security events and electronic accounting meters, including with respect to any patron's device or any other secure interface on a patron's device (such as a smartphone or tablet) that uses a defined protocol.

1.3.3 Software Suppliers and Operators.

The components of a Cashless Wagering System, although they may be constructed in a modular fashion, are designed to work seamlessly together. In addition, Cashless Wagering 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 Wagering 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 test laboratory to facilitate creating a functionally equivalent test environment. Because of the increasingly integrated nature of a Cashless Wagering 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 Wagering System and the individual entities providing them will need to meet such eligibility requirements as the Commission deems appropriate for performance of these requirements.

1.4 Testing and Auditing

1.4.1 Laboratory Testing.

The testing laboratory will test and certify the components of the Cashless Wagering Systems 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 Wagering System is highly dependent upon operational procedures, configurations, and the production environment's network infrastructure. In addition to the testing and certification of Cashless Wagering System components, the Commission may elect to require a periodic operational audit be conducted, using the recommended scope outlined within the appendix for "Operational Audit".

CHAPTER 2: SYSTEM SERVER REQUIREMENTS

2.1 Introduction

2.1.1 General Statement.

A Cashless Wagering System may be entirely integrated into an existing system, such as an electronic monitoring system, or exist as an entirely separate entity. If the Cashless Wagering 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.

2.2 Control Program Requirements

2.2.1 Control Program Self-Verification.

The Cashless Wagering 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 Commission. 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 patron 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.

2.2.2 Control Program Independent Verification.

Each critical control program component of the Cashless Wagering 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 test laboratory, prior to system and/or component approval, shall evaluate the integrity check method.

2.2.3 Shutdown and Recovery.

The Cashless Wagering 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 Commission; and

c) Communication with all components necessary for system operation have been established and similarly authenticated.

2.2.4 Strategic Design.

The Cashless Wagering System shall be designed so that no single failure of any part of the system would cause the loss or corruption of data and that all data is held and able to be accessed or retrieved for the purpose of back-up or audit.

2.2.5 Diagnostic Activity.

All diagnostic activity performed on any cashless terminal or on the Cashless Wagering System generally shall be recorded to include details of the specific terminal, the individual undertaking the diagnostic activity, the results of such diagnostic activity, and the date and time of such activity.

2.3 Cashless Terminal Requirements

2.3.1 General Statement.

The requirements throughout this section apply to cashless terminals, which refer to any machine connected to the Cashless Wagering System, including a gaming machine or kiosk (including betting terminal), that permits a patron to deposit or withdraw cash or make other transactions including those relating to the patron's patron account.

2.3.2 Identifying a Cashless Terminal.

A patron should be able to identify each cashless terminal by a means left to the discretion of the Commission (e.g. remove display menu items that pertain to cashless operation for gaming machines or kiosks not participating; provide a host message indicating cashless capability; or a specific sticker on the gaming machines or kiosk to indicate participation or non-participation).

2.3.3 Patron Identification Components.

A patron identification component is software and/or hardware used with a cashless terminal which supports a means for patrons to provide identification information and/or the source of funds. Patron identification components shall meet the requirements for "Patron Identification Components" as stated within the BCGC-11 Gaming Machine Standards. Examples of these components include card readers, barcode readers, biometric scanners, and wireless devices.

2.4 Communication Requirements

2.4.1 Communications.

The Cashless Wagering 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.

2.4.2 Encryption.

All data transmitted to and from the cashless terminal from the Cashless Wagering System must employ a reasonable level of encryption for the information being transmitted. Additionally, the communication process used by the cashless terminal and the Cashless Wagering 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;

c) Implemented with input data validation controls to ensure that input data is correct;

d) Implemented with processing controls to detect errors in the completeness and accuracy of the processing and update of the Cashless Wagering System; and

e) Implemented with output data controls to ensure the accuracy of information being output or reported.

2.4.3 Cashless Terminal Identification.

The Cashless Wagering System shall uniquely identify each cashless terminal connected to the system. This includes kiosks and any other equipment that are connected to the Cashless Wagering System through a back-office platform or external system.

2.4.4 Monitoring.

The Cashless Wagering System shall be equipped to read and store the applicable significant event and cashless transaction information, and specific cashless meter values from the cashless terminals, as applicable to the system.

2.5 Cashless Transactions

2.5.1 Transaction Identifier.

For all cashless transactions initiated at a cashless terminal, Cashless Wagering Systems shall assign to each transaction a unique identifier of at least eight digits that includes the cashless terminal designation.

2.5.2 Transfer of Funds.

The Cashless Wagering System may provide for and shall account for the transfer of funds from:

a) A patron account through credit transfers directly to a cashless terminal or via the use of TITO technology;

b) A cashless terminal directly to a patron account;

c) A patron account to a wagering instrument for inserting into a cashless terminal; or

d) A wagering instrument to a patron account;

2.5.3 Financial Transactions.

Where financial transactions can be performed automatically by the Cashless Wagering System the following requirements shall be met:

a) The Cashless Wagering System shall require a patron to enter an access code associated with the patron account to initiate any withdrawal or deposit of credits;

b) A deposit into a patron account may be made via a debit instrument transaction, credit card transaction, or other methods which can produce a sufficient audit trail;

c) Funds 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;

d) The Cashless Wagering System shall not permit the transfer of funds to or from a financial institution;

e) The Cashless Wagering System shall not permit the transfer of funds between patron accounts;

f) The Cashless Wagering System shall prohibit withdrawals in excess of that balance; and

g) The Cashless Wagering System shall prohibit simultaneous transactions on a patron account.

2.5.4 Game Play Transactions.

Depending on what is supported by the system and the cashless terminal, the cashless terminal may present transfer options to the patron, which require selection before occurring.

a) Where credits are transferred between the patron account and to the cashless terminal:

   i. Patrons may have the option of moving some or all of their system credit to the cashless terminal they are playing through “withdrawal” from the patron account. Some systems may move either a predefined amount or the patron’s entire balance to the cashless terminal for play;

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

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

iv. When they are finished playing, the patron may have the option to "deposit" their credit balance from the cashless terminal onto their patron 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; and

v. Any credits on the cashless terminal that are attempted to be transferred to the Cashless Wagering System that result in a communication failure for which this is the only available payout medium (the patron cannot cash-out via hopper or printer), must result in a hand-pay lockup or tilt on the cashless terminal.

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

i. A wager shall not be accepted that could cause the patron 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 patron 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 patron funds are wagered.

2.5.5 Transaction Messages.

Cashless Wagering Systems shall cause a relevant, informative message to be displayed to the patron whenever any cashless transaction is being processed. The cashless terminal, patron identification component display, or the patron's device with a secure interface that uses a defined protocol 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; and

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

2.5.6 Transfer of Transactions.

If a patron initiates a financial transaction and that transaction would exceed limits put in place by the operator and/or Commission, this transaction may only be processed provided that the patron is clearly notified that they have withdrawn or deposited less than requested.

2.5.7 Transaction Voids.

The Cashless Wagering System shall limit the ability to void credit transactions to authorized users and approved automated procedures.

2.5.8 Limitations and Exclusions.

The Cashless Wagering System shall provide functionality to permit wagering limits to be set for individual patrons.

a) The Cashless Wagering System shall be able to correctly implement any limitations and/or exclusions put in place by the patron and/or operator as required by the Commission;

b) 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;

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

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

2.5.9 Online Log.

Functionality must exist to allow the Commission to search online an event log for all pending, completed and failed cashless transactions for at least the previous twelve (12) months of data using at the minimum the following search criteria:

a) Date and time range;
b) Cashless terminal; and
c) Patron account number or other unique patron identifier.

2.6 Wagering Instrument Transactions

2.6.1 General Statement.

The following section applies to the use of printed or virtual wagering instruments, such as vouchers and coupons.

2.6.2 Payment by Voucher.

Payment by wagering instrument as a method of credit redemption is only permissible when the applicable requirements established within the “Wagering Instruments” section of the BGC-1 Gaming Machine Standards are met.

2.6.3 Wagering Instrument Information used by the Cashless Terminal.

Validation information shall come from the Cashless Wagering System using a secure communication protocol. The Cashless Wagering System must be able to communicate the following wagering instrument data to the cashless terminal to include on the wagering instrument.

a) Gaming premises name/identification;

b) Indication of an expiration period from date of issue, or date the wagering instrument will expire;

c) Date and time; and

d) Validation number.

2.6.4 Validation Number Generation.

The validation number shall be generated by the Cashless Wagering System or the cashless terminal

a) System Generated. The algorithm or method used by the Cashless Wagering System to generate the wagering instrument validation number must guarantee an insignificant percentage of repetitive validation numbers; and

b) Terminal Generated. The Cashless Wagering System must send a unique seed to the cashless terminal upon enrolling the cashless terminal as wagering instrument capable. The system may subsequently send a new seed to the cashless terminal after a wagering instrument is issued. The algorithm or methods used to determine the seed must guarantee an insignificant percentage of repetitive validation numbers.

2.6.5 Offline Wagering Instrument Issuance

For support of offline wagering instrument issuance, the cashless terminal must be linked to an approved Cashless Wagering System that allows validation of the wagering instrument but does not have to be in constant communication for the issuance of wagering instrument to be permissible:

a) The Cashless Wagering System shall be able to set an expiration length for all provided and still unused validation numbers and seed, key, etc. values. Expired validation numbers and seed, key, etc. values shall be discarded in a way that

prevents the re-use of unique combinations of validation numbers and seed, key, etc. values for a sufficient period of time on the system:

i. Secure seeds, keys, etc. as assigned must be sufficiently random. Measures to avoid predictability will be reviewed by the test laboratory on a case by case basis; and

ii. The minimum length for any secure seeds, keys, etc. employed by the Cashless Wagering System shall be chosen from a pool of the variable type specified by the communication protocol utilized. The pool must be comprised of at least 10 to the power of 14 randomly distributed values.

b) An “offline authentication identifier” shall be included on the wagering instrument. The following minimum set of inputs must be used to create the offline authentication identifier:

i. Cashless terminal identification number or equivalent;

ii. Validation number;

iii. Value of the wagering instrument; and

iv. Secure seed, key, etc. provided by the Cashless Wagering System to the cashless terminal.

2.6.6 Wagering Instrument Issuance during Loss of Communication.

For Cashless Wagering Systems that do not support an offline wagering instrument routine, and communicate to cashless terminal through an Interface Board, if any links between the Interface Board and the database go down, the Interface Board must not respond to the validation request from the cashless terminal and stop wagering instrument issuance, prevent the cashless terminal from further wagering instrument issuance, or not read or store any further wagering instrument information generated by the cashless terminal.

NOTE: A maximum of 2 (two) wagering instruments directly after loss of communication is acceptable, in cases where the interface element has already been ‘seeded’ by the system, provided the wagering instrument issuance information is sent immediately, when communication is reestablished.

2.6.7 Wagering Instrument Redemption.

The Cashless Wagering System must process wagering instrument redemption correctly according to the secure communication protocol implemented.

a) Wagering instruments can be redeemed at cashless terminal which are enrolled for wagering instrument validation with a Cashless Wagering System provided that no credits are issued to the cashless terminal prior to confirmation of wagering instrument validity;

b) If supported, offline wagering instruments can be redeemed at cashier/change booth provided they are enrolled for wagering instrument validation with a Cashless Wagering System and the identification and redemption of offline wagering instruments are supported through a system provided application; and

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

   i. Date and time of status change;

   ii. Status of wagering instrument (i.e. valid, unredeemed, pending, void, invalid, redemption in progress, redeemed, etc.);

   iii. Value of the wagering instrument; and

   iv. The cashless terminal identifying number which issued the wagering instrument.

2.6.8 Cashier Redemption.

Once presented for redemption, the cashier shall scan the bar code via an optical reader or equivalent or input the validation number manually. The Cashless Wagering System shall have the ability to identify and provide a notification in the case of invalid or unredeemable wagering instrument for the following conditions:

a) Wagering instrument cannot be found on file;

b) Wagering instrument record has already been paid; or

c) Amount of wagering instrument differs from amount on file (requirement can be met by display of wagering instrument for confirmation during the redemption process).

2.7 Information to be Maintained

2.7.1 Data Retention and Time Stamping.

The Cashless Wagering 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; and

b) The system shall provide a mechanism to export the data for the purposes of data analysis and auditing/verification (e.g., CSV, XLS).

2.7.2 Patron Account Information.

For each patron account, the information to be maintained and backed up by the System shall include, as applicable:

a) Unique identifying number (patron ID) and username, if different;

b) Personal Identifiable Information (PII) collected by the operator to register a patron and create the account, including:

   i. Full name;

   ii. Any other identifier such as a nickname or alias;

   iii. Date of birth;

   iv. Nationality;

   v. Residential address; and

   vi. Email address and phone number, where available.

c) The following encrypted PII:

   i. Government identification number (social security number, taxpayer identification number, passport number, or equivalent);

ii. Authentication credential (password, PIN, etc.); and

iii. Details of a bank account or credit account in the name of the patron, for paying and receiving funds.

d) The date and method of identity verification, including, where applicable, a description of the photographic ID or other identification credential provided by a patron to confirm their identity and its date of expiration;

e) If the patron account will be connected to a Cashless Wagering System or other account, the kinds of gaming to which the account will relate (physical gaming, eGaming, etc.);

f) The date and time the patron account was opened and, as applicable, activated and closed;

g) The date and time the patron first and last accessed his account, including IP address;

h) The date of patron agreement to the operator's terms and conditions and privacy policy;

i) Account details and current balance, including any incentive credits. All non-cashable credits and incentive credits that have a possible expiration shall be maintained separately;

j) Previous accounts, if any, and reason for de-activation;

k) The method from which the account was registered;

l) Exclusions/limitations information as required by the Commission:

i. The date and time of the request (if applicable);

ii. Description and reason of exclusion/limitation;

iii. Type of exclusion/limitation (e.g., operator-imposed exclusion, self-imposed deposit limitation);

iv. The date exclusion/limitation commenced; and

v. The date exclusion/limitation ended (if applicable).

m) The details of all transactions relating to the account, including any adjustments to the account:

i. Type of transaction (e.g., deposit, withdrawal, adjustment);

ii. The date and time of the transaction;

iii. Unique transaction number;

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 unique cashless terminal ID which handled the transaction (if applicable);

viii. Transaction status (pending, complete, etc.);

ix. Method of deposit/withdrawal (e.g., cash, personal check, cashier's check, wire transfer, money order, debit instrument, credit card, electronic funds transfer, etc.);

x. Deposit authorization number; and

xi. The physical location of the patron while accessing the patron account (where such information is available).

n) The current status of the patron account (e.g., active, dormant, closed, excluded, etc.).

2.7.3 Wagering Instrument Information.

The Cashless Wagering System shall record a log in relation to each wagering instrument which shall include:

a) Unique validation number;

b) Type of transaction or other method of differentiating wagering instrument types (assuming multiple types are available);

c) Value of the wagering instrument;

d) Indication of an expiration period from date of issue, or date the wagering instrument will expire;

e) Date and time the wagering instrument was issued;

f) The cashless terminal identifying number which issued the wagering instrument;

g) Date and time the wagering instrument was redeemed or voided (blank until known);

h) The cashier/change booth or cashless terminal identifying number which redeemed or voided the wagering instrument (blank until known); and

i) Status of wagering instrument (i.e. valid, unredeemed, pending, void, invalid, redemption in progress, redeemed, etc.).

2.7.4 Incentive Information.

For Cashless Wagering Systems which support incentive awards that are redeemable wagering credits, or merchandise, the information to be maintained and backed up for each incentive offered shall include:

a) The date and time the incentive award period started and ended or will end (if known);

b) Current balance for incentive awards;

c) Total amount of incentive awards issued;

d) Total amount of incentive awards redeemed;

e) Total amount of incentive awards expired;

f) Total amount of incentive award adjustments; and

g) Unique ID for the incentive award.

2.7.5 Transaction Information.

The Cashless Wagering System shall record a log in relation to each cashless transaction which shall include:

a) Type of transaction;

b) Monetary value of transaction;

c) Time and date of transaction;

d) Patron details, where available;

e) The unique transaction number;

f) The cashless terminal identifying number; and

g) Any other information the Commission may by written direction require.

2.7.6 Void Information.

The Cashless Wagering System shall record a log in relation to each void which shall include:

a) the person or procedure that voided the record;

b) the patron account number;

c) the unique transaction number;

d) the date and time the void occurred; and

e) the value of the transaction.

2.7.7 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 incentive parameters, if supported by the system;

f) Adjustments to a patron account balance;

g) Changes made to patron data and sensitive information recorded in a patron account;

h) Deactivation of a patron account;

i) Large financial transactions (single and aggregate over defined time period) in excess of a value specified by the Commission, if supported by the system;

j) Irrecoverable loss of sensitive information;

k) Any other activity requiring user intervention and occurring outside of the normal

scope of system operation; and

l) Other significant or unusual events as deemed applicable by the Commission.

2.8 Reporting Requirements

2.8.1 General Reporting Requirements.

The Cashless Wagering System shall be capable of generating the information needed to compile financial reconciliation and variance reports as may be required by the legislation or by written direction of the Commission 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 Commission 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 premises and/or operator (or other identified), the selected interval and the date/time the report was generated;

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

   iii. Labeled fields which can be clearly understood in accordance with their function.

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

2.8.2 Daily Transaction Reports.

The System shall be able to provide the following information needed to create one or more daily reports containing the following, as applicable:

a) For each credit transaction on a cashless terminal:
   i. The individual amount of each credit transaction;
   ii. The date and time of each credit transaction;
   iii. The unique transaction number of each credit transaction; and
   iv. The total amount of all credit transactions.

b) For each transaction that relates to a non-cashable credit on a cashless terminal:
   i. The individual amount of each non-cashable credit transaction;
   ii. The date and time of each non-cashable credit transaction;
   iii. The unique transaction number of each non-cashable credit transaction; and
   iv. The total amount of all non-cashable credit transactions.

c) For each credit withdrawal from a patron account:
   i. The individual amount of each credit withdrawal;
   ii. The date and time of each credit withdrawal;
   iii. The unique transaction number of each credit withdrawal; and
   iv. The total amount of all credit withdrawals.

d) For each credit deposit to a patron account:
   i. The individual amount of each credit deposit;
   ii. The date and time of each credit deposit;
   iii. The unique transaction number of each credit deposit; and
   iv. The total amount of all credit deposit.

2.8.3 Financial and Patron Reports.

The Cashless Wagering System shall be able to produce the following financial and patron reports:

a) Cashless Wagering System Activity Reports. These reports are to include deposits, transfers to and from cashless terminals, withdrawals, adjustments and

balances, by patron account. For wagering instruments, these reports are to also include all wagering instruments generated by a cashless terminal and all wagering instruments redeemed by the cashier/change booth or other cashless terminals;

b) Liability Reports. 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 incentive value (where supported), and the current day's ending cashless liability, if applicable. For wagering instruments, these reports are to also include liabilities by date issued and by sequence number. Separate reports may be generated for incentive and non-incentive cashless liability;

c) Reconciliation Summary and Variance Reports. These reports will reconcile each cashless terminal's meter(s) against the system's activity, by cashless terminal and by type of transaction, as applicable;

d) Cashier Summary and Detail Reports. These reports shall include patron account, deposits and withdrawals, amount of transaction, date and time of transaction. patron account, and cashier starting and ending balances, session start and end date/time (etc.) by cashier. For wagering instruments, these reports are to also include details on individual wagering instruments, the sum of the wagering instruments paid by cashier/change booth;

e) Significant Event Reports. 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.

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

2.8.4 Wagering Instrument Reporting Requirements.

The following additional reports shall be generated at a minimum and reconciled with all validated/redeemed wagering instruments:

a) Wagering Instrument Issuance Reports. These reports are to include for each wagering instrument the date issued, amount, sequence number and identification of cashless terminal where issued;

b) Wagering Instrument Redemption Reports. These reports are to include redemptions by date and means of redemption (e.g., cashless terminal, cashier/change booth, etc.);

c) Wagering Instrument Count Reports. These reports are to include all wagering instruments counted in the count room, by cashless terminal and by type of wagering instrument;

d) Wagering Instrument Expiration Reports. These reports are to include all wagering instruments expired by date issued, sequence number and identification of cashless terminal where issued; and

e) Wagering Instrument Void Reports. These reports are to include all wagering instruments voided by date issued, instrument sequence number and identification of cashless terminal where issued.

CHAPTER 3: PATRON ACCOUNT REQUIREMENTS

3.1 Introduction

3.1.1 General Statement.

The following chapter applies to patron accounts and cashless transactions in addition to the “Patron Account Controls” section within this document.

NOTE: Patron account registration and verification are required by the System for a patron to participate in gaming by means of eGaming.

3.2 Patron Account Access and Maintenance

3.2.1 Patron Authentication.

All cashless transactions between a supporting cashless terminal and the Cashless Wagering System must be secured using a method of authentication, such as insertion of a card into a magnetic card reader, username and password or a secure alternative means approved by the Commission by written direction (e.g., debit instrument or card insertion or “tap” (contactless) capacity on the patron identification component, a similar approved process that allows for the identification of the patron and the source of funds if a software application on a patron’s device is used). Authentication methods are subject to the discretion of the Commission as necessary. The requirement does not prohibit the option for more than one method of authentication being available for a patron to access their account.

a) If the system does not recognize the authentication credentials provided by the patron, an explanatory message shall be displayed to the patron which prompts the patron to try again;

b) Where a patron has forgotten their authentication credentials, a multi-factor authentication process shall be employed for the retrieval or reset of their authentication credentials, which shall use no less than two of the following to verify a patron’s identity:

   i. Information known only to the patron, such as a password, pattern or answer to a question;

   ii. An item possessed by the patron such as an electronic token, physical token or identification card; or

   iii. The patron’s biometric data such as fingerprints, facial or voice recognition.

c) Current account balance information, including any incentive credits, and transaction options shall be available to the patron once authenticated:

   i. All non-cashable credits and incentive credits that have a possible expiration shall be indicated separately; and

   ii. This information must be available on demand from any terminal on which the patron is wagering.

d) The Cashless Wagering System shall provide functionality to allow for:

i. A lost or stolen patron account or other magnetic strip card to be blocked and for any attempt to use such a card to be reported; and

ii. An account to be locked in the event that suspicious activity is detected, such as three consecutive failed access attempts in a thirty-minute period. A multi-factor authentication process shall be employed for the account to be unlocked.

e) The Cashless Wagering System may also provide for the use of a magnetic strip player card (other than those connected to the patron account) onto which credit may be added for use in gaming and which may only be cashed out at the cage.

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

3.2.2 Smart Card/Device Technology.

If approved by the Commission, patrons 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 Wagering System's database. Smart cards/devices which have the ability to maintain a patron account balance are only permissible when the Cashless Wagering 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.

3.2.3 Patron Inactivity.

For patron accounts accessed remotely for gaming or account management, after thirty minutes of inactivity on that Cashless Terminal, or a period determined by the

Commission, the patron shall be required to re-authenticate to access their patron account.

a) No further gaming or financial transactions on that device are permitted until the patron has been re-authenticated; and

b) A simpler means may be offered for a patron to re-authenticate on that device, such as operating system-level authentication (e.g., biometrics) or a Personal Identification Number (PIN). Each means for re-authentication will be evaluated on a case-by-case basis by the testing laboratory:

   i. This functionality may be disabled; and

   ii. Once every thirty days, or a period specified by the Commission, the patron will be required to provide full authentication on that device.

NOTE: When the operator establishes basic one-way communications where the patron's behavior is expected to be passive (i.e. transmission of a live sporting event), the patron will be considered to remain active, even if no action is taking place.

3.2.4 Modification of Patron Information.

The system shall allow the ability to update authentication credentials, registration information and the account used for financial transactions for each patron:

a) A multi-factor authentication process shall be employed for these purposes;

b) The system shall maintain a record of any changes to the access code associated with a patron account including the date and time when the change was made and the location where the change was made; and

c) The system shall record all other changes to the patron account, including who made or authorised the change, the details of the change, and the time and date of the change.

3.2.5 Accounts and Sub-Accounts.

A patron shall only be permitted to have one active patron account at a time unless specifically authorized by the Commission:

a) A patron account shall comprise the following sub-accounts:

   i. a general account; and

   ii. a separate account for each of the following types of gaming that the account covers:

      (A) physical gaming; and

      (B) gaming by means of eGaming;

b) No payments by the patron may be made into one of the separate accounts except by transfer from the general account;

c) The operator shall not permit a patron to engage in eGaming except by using an appropriate sub-account; and

d) The operator shall not permit a patron to draw on a patron account except for the purchase of chips or engaging in gaming, or eGaming.

3.2.6 Maximum Balance Limits.

The Cashless Wagering System must enforce a maximum balance limit on the patron account.

a) Deposits may not occur which cause the patron account balance to exceed this limit; and

b) If the patron 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.

3.2.7 Transaction Log or Account Statement.

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

a) Deposits to the patron account;

b) Withdrawals from the patron account;

c) Credits added to/removed from the patron account from game play, the details of any bets made by the patron through the account including winnings;

d) Incentive credits added to/removed from the patron account;

e) Manual adjustments or modifications to the patron account (e.g., due to refunds);

f) Any other additions to, or deductions from, the patron account, that would not otherwise be metered under any of the above listed items; and

g) A statement of the remaining balance in the account and the proportion of the balance that represents the winnings.

3.3 Access to Patron Account Remotely

3.3.1 General Statement.

Depending on the implementation(s) approved by the Commission, a patron may be allowed to access their patron account and/or perform financial transactions remotely directly using an approved secure interface that uses a defined protocol or a similar application or software package on a patron's device. Examples of a patron's device include a personal computer, mobile phone, tablet, etc.

NOTE: Nothing in this section should be interpreted as being applicable to gaming *by means of eGaming using a patron's device.*

3.3.2 Software Identification.

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

3.3.3 Device-System Interactions.

The patron may obtain/download an application or software package or access the software via a browser to access their patron account on the Cashless Wagering System:

a) Patrons 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 patron'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; and

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.

3.3.4 Compatibility Verification.

During any installation or initialization and prior to commencing patron account access, the software used in conjunction with the Cashless Wagering System shall detect any incompatibilities or resource limitations with the patron'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 patron account access and display an appropriate error message.

3.3.5 Software Content.

The software shall not contain any malicious code or functionality deemed to be malicious in nature by the Commission. 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.

3.3.6 Cookies.

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

3.3.7 Information Access.

The items specified in the “Information for Patron Accounts” section of this document shall be displayed, either directly from the patron’s device screen or from a page accessible to the patron:

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

b) The display of this information shall be adapted to the patron’s device. For example, where a patron’s device uses technologies with a smaller display screen, it is permissible to present an abridged version of the information accessible directly from within the patron’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.

3.4 Patron Loyalty Programs

3.4.1 Patron Loyalty Programs.

Patron loyalty programs are any programs that provide incentive awards for patrons, typically based on the volume of play or revenue received from a patron. If patron loyalty programs are supported by the Cashless Wagering System, the following principles shall apply:

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

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

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

APPENDIX A: OPERATIONAL AUDIT

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 the Commission, will be reviewed in an periodic operational audit, including, but not limited to, patron account management, review of the operational processes that are critical to compliance, storing and/or processing patron data, handling various financial transactions, fundamental practices relevant to the limitation of risks, and any other objectives established by the Commission.

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 Commission within their rules, regulations, and internal controls.

A.2 General Operating Procedures

A.2.1 Internal Control Procedures.

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

a) The internal control document shall set out:
   i. How a patron account and its sub-accounts will be operated;
   ii. Circumstances in which a patron account and each kind of sub-account may be used, or must be used;
   iii. Any restrictions that may be, or shall be, placed on who may hold a patron account or the use of a patron account or sub-account;
   iv. How a patron will be given access to the patron account and any sub-accounts;
   v. Mechanisms to ensure that, as far as possible, account holders remain contactable; and
   vi. Procedures for closing a patron account, and for dealing with dormant accounts.

b) In addition, the internal control document shall contain details on its risk management framework, including but not limited to:
   i. Automated and manual risk management procedures;
   ii. Employee management, including access controls and segregation of duties;
   iii. Information regarding identifying and reporting fraud and suspicious conduct;
   iv. Controls ensuring regulatory compliance;
   v. Description of Anti-Money Laundering (AML) compliance standards including procedures for detecting structuring to avoid reporting requirements;

vi. Description of all software applications that comprise the Cashless Wagering System;

vii. Description of all integrated third-party service providers; and

viii. Any other information required by the Commission.

A.2.2 Operator Reserves.

The operator shall have processes in place for maintaining and protecting adequate cash reserves, as determined by the Commission, including segregated accounts of funds held for patron accounts and operational funds.

a) The operator shall maintain all funds held by it on behalf of patrons in patron accounts separately from the funds of the gaming premises and in a bank. These funds include:

i. Cleared funds deposited with the operator;

ii. Winnings or prizes which the customer has chosen to leave on deposit with the operator; and

iii. Any loyalty or other bonuses or credits that are due but unpaid.

b) The operator shall not have any recourse to the funds standing to the credit of a patron, except:

i. To make payment to the patron of such funds as the patron wishes to withdraw from his patron account;

ii. To debit funds required for gaming transactions in accordance with any provisions of the internal control document governing electronic gaming or cashless wagering systems;

iii. To make adjustments following resolution of a dispute, provided that the operator has given written notification of the adjustment in advance;

iv. To debit inactive funds in accordance with the terms and conditions of the patron account as accepted by the patron and in accordance with the internal control document;

v. As may be permitted by the legislation;

vi. On the instruction of the Commission; or

vii. As may be required by law.

A.2.3 Protection of Patron Funds.

The operator shall keep and maintain separate accounts, as approved by the Commission, at a bank for use for all banking transactions arising in relation to the operator. The operator shall have processes in place to ensure funds in an operator account are either to be held in trust for the patron in a segregated account or in a special purpose segregated account that is maintained and controlled by a properly constituted corporate entity that is not the operator and whose governing board includes one or more corporate directors who are independent of the operator and of any corporation related to or controlled by the operator. In addition, the operator shall have procedures that are reasonably designed to:

a) Ensure that funds generated from 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 patron whose funds are being held;

c) Prevent commingling of funds in the segregated account with other funds including, without limitation, funds of the operator;

d) Ensure that all patrons are informed as to the level of protection (if any) of funds held by the operator in the event of the insolvency of the operator; and

e) From time to time provide the Commission, as required, and in a form approved by the Commission, with a written authority addressed to the bank authorizing the bank to comply with any requirements of an inspector exercising the powers conferred by this section.

A.2.4 Complaint/Dispute Process.

The operator shall provide a method for a patron to make a complaint/dispute, and to enable the patron to notify the Commission if such complaint/dispute has not been or cannot be addressed by the operator, or under other circumstances as specified by the law of the Commission.

a) Patrons shall be able to log complaints/disputes on a 24/7 basis;

b) The internal control document shall contain a documented process between the operator and the Commission on the complaint/dispute reporting and resolution process, including:

   i. How patrons can make complaints;

   ii. Mechanisms for dealing different kinds of complaints and disputes; and

   iii. How complaints and disputes are to be reported to and reviewed by the compliance committee.

c) The operator shall ensure that:

   i. The gaming premises at all times has a member of staff present with authority to resolve complaints up to a maximum amount specified in the internal control document;

   ii. The gaming premises at all times has a member of the staff with authority to resolve complaints above that amount available to be called on; and

   iii. A record is kept of all correspondence relating to complaints for a period of five years and provided to the compliance committee at such regular intervals as the compliance committee requires.

d) Upon receipt of a complaint, if the complaint is not resolved immediately, the operator shall:

   i. Record the details of the complaint;

   ii. If the information is not already available on a patron account, record the full name, address and contact details of the complainant;

   iii. If the complaint is a gaming complaint made by a patron, draw to the attention of the patron the matters in the house rules; and

   iv. Provide the patron with such documentation or further information as is required by the internal control document or a written direction by the Commission.

e) If a patron refuses to provide his name and contact details, the operator shall record the details of the complaint and a description of the complainant;

f) If a gaming complaint that relates to an amount of $500 or more is not resolved to the satisfaction of the patron, the operator shall:

   i. Inform the patron that the operator is unable to resolve the complaint;

ii. Inform the patron of his rights to request that an inspector conduct an investigation into the dispute;

iii. Provide the patron with a card or other document approved by the Commission that sets out the patron's rights and includes the address and contact details of the Commission; and

iv. Notify an Inspector of the dispute.

g) The operator shall seek to resolve all complaints in good faith; and

h) The operator shall ensure that it complies with the requirements of this section, even if the complaint appears to be frivolous or vexatious.

A.2.5 Responsible Gaming.

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

A.3 Patron Account Controls

A.3.1 Registration and Verification.

Patron accounts shall be maintained electronically:

a) The operator must employ a mechanism to collect (either through the Cashless Wagering System or via a manual procedure approved by the Commission) the following patron details prior to the registration of a patron account:
   i. Full name;
   ii. Any other identifier such as a nickname or alias;
   iii. Date of birth;
   iv. Nationality;
   v. Residential address;
   vi. Details of a bank account or credit account in the name of the patron, for paying and receiving funds;
   vii. Email address and phone number (where available); and
   viii. Any other information that the Commission by written direction requires.

b) The operator shall not permit a patron account to be held:
   i. Anonymously;
   ii. In a fictitious name;
   iii. By a patron who already holds another patron account;
   iv. By a person under 18 years of age; or
   v. By an excluded person.

c) During the registration process, the patron shall:
   i. Be denied the ability to register for a patron account if they submit a birth date which indicates that they are under 18 years of age;
   ii. Be informed on the registration form which information fields are “required”, which are not, and what will be the consequences of not filling in the required

fields; and

iii. Agree to the terms and conditions and privacy policy.

d) The patron must, by signing an appropriate statement, agree that the patron:

i. Has provided accurate patron details;

ii. Will not allow another person to use his patron account;

iii. Will place bets only on his own behalf and not on behalf of any other person;

iv. Is bound by the dispute resolution procedures established by the Commission and agrees to submit to arbitration in the event of an appeal;

v. Is subject to the house rules of the operator;

vi. Is subject to any applicable terms and conditions, including provisions relating to dealing with dormant accounts;

vii. Consents to Bermuda as the exclusive jurisdiction for the resolution of all disputes as between the patron and the operator; and

viii. Consents to the patron details and the details of the patron's transactions being recorded by the operator and made available to the Commission.

e) Identity verification shall be undertaken before a patron is allowed to place a bet. Third-party identity verification service providers may be used for identity verification as approved by the Commission:

i. Identity verification shall authenticate the legal name, residential address, and date of birth of the individual at a minimum as required by the Commission;

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

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

f) The patron account can only become active once age and identity verification are successfully completed, the patron is determined to not be under 18 years of age or on any exclusion lists or prohibited from establishing or maintaining an account for any other reason, the patron has acknowledged the necessary terms and conditions and privacy policy, and the patron account registration is complete. The operator shall not activate a patron account, unless:

i. The patron has appeared at the gaming premises in person;

ii. The operator is satisfied as to the identity of the person;

iii. The operator holds the patron details about the patron, and is satisfied that it is correct; and

iv. The patron has signed the statement mentioned in paragraph (d).

g) The operator shall at intervals of not more than 12 months request a patron to update any of the patron details that have changed in order to ensure that the patron's information obtained remains current and accurate.

A.3.2 Fraudulent Accounts.

The operator shall have a documented public policy for the treatment of patron 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 patron providing access to persons under 18 years of age; and

c) The handling of deposits, wagers, and wins associated with a fraudulent account.

A.3.3 Patron Data Security.

Any information obtained in respect to the patron account, including patron data and authentication credentials, shall be done in compliance with the privacy policy and local privacy regulations and standards observed by the Commission. Both patron data and the patron funds shall be considered as critical assets for the purposes of risk assessment. In addition:

a) Any patron 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 patron account;

ii. The amount of money wagered by a particular patron on any game or cashless terminal;

iii. The account number and authentication credentials that identify the patron; and

iv. The name, address, and other information in the possession of the operator that would identify the patron to anyone other than the Commission or the operator.

b) There shall be procedures in place for the security and sharing of patron data, funds in a patron account and other sensitive information as required by the Commission, 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 Commission.

A.3.4 Player Funds Maintenance.

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

a) Where such financial transactions cannot be performed automatically by the Cashless Wagering 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 patron nor allow the deposit of funds into a patron 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 patron account, the operator is awaiting actual receipt of such funds in the ordinary course of business;

d) The operator shall not allow a patron account to be overdrawn or maintain a negative balance unless caused by payment processing issues outside the control of the operator;

e) The operator shall not permit a transfer from a patron account to an account outside the gaming premises other than to a bank account or credit card account in the patron’s name;

f) A patron’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, provided that:

   i. The request is made in accordance with the terms and conditions applicable to the patron account;

   ii. There is no ongoing or pending dispute lodged with the Commission the outcome of which may impact on the funds held in the patron account; and

   iii. The operator has not been directed by the Commission to withhold payments from the account.

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

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

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 patron data, including any sensitive information given by the patron or transaction related data;

d) There shall be an established procedure for assuring the match of ownership between the payment type holder and the patron account holder;

e) The operator shall generate all transactional records of patron accounts. The data recorded shall allow the operator to trace a single financial transaction of a patron from another transaction;

A.3.6 Limitations.

Patrons shall be provided with a method to impose limitations for gaming parameters including, but not limited to those specified within this section. There shall also be a method for the operator to impose any limitations for gaming parameters as required by the Commission.

a) The operator shall implement functionality where the patron is able to set limits on the following gaming parameters:

   i. The amount the patron may deposit or use to purchase chips during a specific period;

   ii. The amount a patron may lose during a specified period or in relation to a specified number of transactions;

   iii. The amount a patron may wager during a specific period or in relation to a specific number of transactions;

   iv. The ability of a patron to engage in eGaming;

   v. The time spent on the game; and

   vi. The amount withdrawn during a gaming session.

b) Once established by a patron 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 Commission;

c) Patrons 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 patron;

d) 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 patron;

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

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

A.3.7 Exclusions.

Patrons shall be provided with a method to exclude themselves from gaming for a specified period or indefinitely, as required by the Commission. If supported, there shall also be a method for the operator to exclude a patron from gaming as required by the Commission:

a) Patrons 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 patron, until the exclusion has been removed;

c) While excluded, the patron 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;

d) All advertising or marketing material shall not specifically target patrons that have been excluded from play; and

e) The operator may establish procedures to evaluate requests made by third-parties to exclude a patron from gaming, including when the requestor provides

documentary evidence of sole or joint financial responsibility for the source of funds deposited with an operator by the patron or a court order requiring the patron to pay unmet financial obligations (e.g., child support).

A.3.8 Promotional Message Exclusion.

Patrons must have the option to unsubscribe from promotional or other advertising materials.

A.3.9 Dormant Accounts.

A patron account is considered to be dormant if it has had no patron-initiated activity for period of 12 months as specified in the terms and conditions:

a) Upon an account becoming dormant, the operator shall seek to establish whether the patron wishes to continue the account and shall continue to do so at regular intervals thereafter;

b) Procedures shall be in place to:

   i) Allow access by patron to their inactive account only after performing additional identity verification;

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

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

c) If the operator has not been able to contact the patron within one month after the account became dormant, and the account has $20 or less in funds, the operator may close the account;

d) If the operator has not been able to contact the patron within 12 months after the account became dormant, the operator may close the account; and

e) A operator shall notify the Commission 14 days prior to closing any patron account, and shall take such steps as the Commission directs, including transferring any funds in the patron account to the Commission or to such other account as the

Commission directs.

A.3.10 Account Closure.

Patrons shall be provided with a method to close their patron account at any time unless an account is closed due to being dormant, the following shall apply:

b) An operator shall close a patron account:
   i. On request by a patron;
   ii. On instruction to do so by the Commission; and
   iii. On the patron becoming an excluded person.

c) The internal control document may specify a form or forms for a request to close a patron account but must allow for a request to be made remotely;

d) Upon closing a patron account:
   i. The operator shall provide the patron with a closing statement detailing all payments made into or from the patron account; and
   ii. All funds shall be returned to the patron by way of balance transfer to a bank account or credit card account in the name of the patron, provided that the operator acknowledges that the funds have cleared.

A.4 Information for Patron Accounts

A.4.1 General Statement.

The following requirements apply to information displays for a patron account, and/or information regarding a patron account that is otherwise provided to patrons via external signage, forms, or brochures available at the gaming premises.

A.4.2 Terms and Conditions.

A set of terms and conditions shall be available to the patron. During the registration process and when any terms and conditions are materially updated (i.e., beyond any grammatical or other minor changes), the patron shall agree to the terms and conditions. The terms and conditions shall:

a) State that only individuals legally permitted by their respective jurisdiction can participate in gaming;

b) Advise the patron to keep their authentication credentials (e.g., password and username) secure;

c) Disclose all processes for dealing with lost authentication credentials, forced changes, password strength and other related items required by the Commission;

d) Specify the conditions under which an account is declared dormant and explain what actions will be undertaken on the account once this declaration is made;

e) Clearly define what happens to the patron's pending bets placed prior to any self-imposed or operator-imposed exclusion, including the return of all bets, or settling all bets, as appropriate;

f) Contain information about timeframes and limits regarding deposits to and/or withdrawals from the patron account, including a clear and concise explanation of all fees (if applicable);

g) Disclose the operator's policy regarding the acceptance of debit instruments, and electronic funds transfer to the patron;

h) State that the operator has the right to:

i. Refuse to establish a patron account for what it deems good and sufficient reason;

ii. Refuse deposits to and withdrawals from patron accounts for what it deems good and sufficient reason; and

iii. Unless there is a pending investigation or patron dispute, suspend or close any patron account at any time pursuant to the terms and conditions between the operator and the patron.

A.4.3 Privacy Policy.

A privacy policy shall be available to the patron. During the registration process and when the privacy policy is materially updated (i.e., beyond any grammatical or other minor changes), the patron shall agree to the privacy policy. The privacy policy shall state:

a) The personally identifiable information (PII) required to be collected;

b) The purpose and legal basis for PII collection and of every processing activity for which consent is being sought including, where required by the Commission, the "legitimate interest" pursued by the operator (or third-party service provider(s)) if this is the legal basis chosen (i.e., identification of the specific interest in question);

c) The period in which the PII is stored, or, if no period can be possibly set, the criteria used to set this. It is not sufficient for the operator to state that the PII will be kept for as long as necessary for the legitimate purposes of the processing;

d) The conditions under which PII may be disclosed;

e) An affirmation that measures are in place to prevent the unauthorised or unnecessary disclosure of the PII;

f) The identity and contact details on the operator who is seeking the consent, including any third-party service provider(s) which may access and or use this PII;

g) Where required by the Commission, that the patron has a right to:

   i. Access, export, or transfer their PII;

   ii. Rectify, erase, or restrict access to their PII;

   iii. Object to the PII processing; and

   iv. To withdraw consent, if the processing is based on consent.

h) The rights and possibility of a patron to file a complaint to the Commission;

i) For PII collected directly from the patron, whether there is a legal or contractual obligation to provide the PII and the consequences of not providing that PII;

j) Where applicable and required by the Commission, information on the operator's use of automated decision-making, including profiling, and at least in those cases, without hindering compliance with other legal obligations:

   i. Sufficient insight into the logic of the automated decision-making;

   ii. The significance and the envisaged consequences of such processing for the patron; and

   iii. Safeguards in place around solely automated decision-making require, including information for a patron on how to contest the decision and to require direct human review or intervention.

A.4.4 Patron Protection Information.

The operator shall maintain an online patron protection page that is accessible to a patron via the gaming premises website at all times without the requirement to log on to a patron account. The patron protection page shall include the following:

a) Any message that the Commission may by written direction require;

b) Information about potential risks associated with excessive gaming;

c) A prominent direct link to at least one organisation dedicated to helping people with potential gambling problems, including one based in Bermuda if available;

d) A clear statement of the operator's policy and commitment to responsible gaming;

e) A statement that no persons under 18 years of age are permitted to participate in gaming;

f) Information on the following matters, or a prominent direct link to such information from an organisation dedicated to helping people with potential gambling problems:

   i. Practical tips to stay within safe limits;

   ii. Myths associated with gambling;

iii. The risks associated with gambling; and

iv. The signs of a potential gambling problem.

g) Rules governing self-imposed responsible gaming limits and measures, including the patron's right to set responsible gaming limits, self-exclude, or suspend their account, as well as information on how to invoke those limits and measures;

h) For patron accounts:

i. a method for the patron to obtain account and wager or bet history from the operator;

ii. mechanisms in place which can be used to detect unauthorised use of their account, such as reviewing financial statements against known deposits; and

iii. prominent links to information relating to responsible gaming and problem gambling.

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

j) Contact information for the Commission and/or a link to their website.

NOTE: For gaming by means of eGaming, all links to problem gambling services provided by third parties are to be regularly tested by the operator. Gaming by means of eGaming may not occur where the links used to supply information on patron protection are not displayed or are not operational. Where the link is no longer available or not available for a significant period of time, the operator shall provide an alternative support service.

A.4.5 Incentive Awards.

If supported in the cashless environment, an operator may offer incentive awards, which are credits and/or prizes not included in the paytable of a game and are based upon predetermined events or criteria established by the parameters of the Cashless Wagering System:

a) Patrons shall be able to access clear and unambiguous terms and conditions pertaining to any available incentive award offers, which shall include the following at a minimum:

i. The date and time presented;

ii. The date and time the offer is active and expires;

iii. Patron eligibility, including any limitations on participation;

iv. Any restriction or terms on withdrawals of funds;

v. Wagering requirements and limitations by type of event or wager type, game, game theme and/or paytable;

vi. How the patron is notified when they have received an incentive award;

vii. The order in which funds are used for wagers; and

viii. Rules regarding cancellation.

b) An operator shall provide a clear and conspicuous method for a patron to cancel their participation in an incentive award offer that utilizes non-cashable credits.

i. Upon request for cancellation, the operator shall inform the patron of the amount of cashable patron funds that will be returned upon cancellation and the value of non-cashable incentive credits that will be removed from the patron account; and

ii. If the patron elects to proceed with cancellation, cashable patron funds remaining in a patron account shall be returned in accordance with the terms of the offer.

c) Once a patron has met the terms of an incentive award offer, the operator shall not limit winnings earned while participating in the offer (i.e., the non-cashable credits of the offer will be added to the cashable patron funds).

A.5 Technical Security Controls

A.5.1 Operating Protocol.

An operating protocol shall be in place which sets out how the Cashless Wagering System will be operated in the gaming premises, including:

a) A detailed description of the Cashless Wagering System and of its scope and functions in the gaming premises;

b) Rules on who may access the system and the actions that may be performed;

c) Checks and security protocols; and

d) Rules and procedures for connecting or adapting the Cashless Wagering System to any new or changed cashless terminals or other gaming equipment.

A.5.2 Physical Location of Components.

The Cashless Wagering System servers and databases shall be held in a restricted and secure area which shall be on the gaming premises unless otherwise agreed in writing by the Commission. The restricted and secure area 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 Commission.

A.5.3 Logical Access Control.

The cashless environment shall be logically secured against unauthorized access by authentication credentials approved by the Commission, such as passwords, multi-factor authentication, digital certificates, PINs, biometrics, and other access methods (e.g., magnetic swipe, proximity cards, embedded chip cards):

a) The Cashless Wagering System shall restrict access by employees in accordance with job functions and responsibilities, shall prevent access by unauthorized parties, and shall detect possible unauthorized access and mitigate to the greatest extent possible the information accessible;

b) The number of users that have the requisite permissions to adjust critical parameters shall be limited;

c) All network hubs, services and connection ports shall be secured to prevent unauthorized access to the network;

d) The number of workstations where critical cashless applications or associated databases may be accessed shall be limited; and

e) Procedures shall be in place to identify and flag suspect patron and employee accounts to prevent their unauthorized use to include:

   i. Having a maximum number of three successive incorrect attempts at authentication before account lockout;

   ii. Flagging of suspect accounts where authentication credentials may have been stolen;

   iii. Invalidating accounts and cards and transferring balances into a new account;

   iv. Establishing limits for maximum cashless activity or overall wagering activities in and out as a global or individual variable to preclude money laundering; and

   v. Implementing a means by which the use of deactivated or flagged accounts/cards are reported to the operator.

A.5.4 Remote Access Requirements.

The Cashless Wagering System may permit remote access by an authorised staff member of an approved gaming supplier (a “remote user”), provided that:

a) The Cashless Wagering System and the operating protocol ensure a secure means of authentication of the identity of remote user;

b) The connection is established in a way that prevents unauthorized access to the system or the data transmitted between the remote user and the Cashless Wagering System;

c) A firewall or equivalent protection is used by the operator in conjunction with the connection; and

d) All access and transactions by a remote user are recorded by the Cashless Wagering System, including:

   i) date and time of access;

   ii) the identity of the remote user;

   iii) any user accounts accessed during the remote session;

   iv) the reason for access; and

   v) details of any modifications or transactions.

A.5.6 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.5.7 Data Alteration.

The alteration of any accounting, reporting or patron 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.5.8 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.5.9 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 six years. 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 Wagering 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.5.10 Uninterruptible Power Supply (UPS) Support.

All components in the cashless environment shall be provided with adequate primary power. Where the Cashless Wagering 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.5.11 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 Commission:

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 Wagering 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 Commission to guarantee that no vulnerabilities putting at risk the security and operation of the Cashless Wagering System exist; and

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

A.6 Currency Transaction Reports

A.6.1 Currency Transaction Reports.

The following requirements apply for currency transaction reports:

a) The operator shall maintain a record of all single transactions in which a patron either provides to or removes from the operator the following amounts, irrespective of whether such amount is made up of cash, wire transfers, cheque or other negotiable instrument or a combination of these:
   i. $10,000 or more for casino operators.

b) A record maintained in accordance with this section shall be verified by the operator and shall include the following information:
   i. The name of the patron;
   ii. The residential address of the patron, or in the case of a patron not resident in Bermuda his temporary Bermuda address and his overseas residential address; and
   iii. The date of birth of the patron.

c) A series of related transactions in any 24-hour period or the aggregate of transactions for any one patron in any 24-hour period shall be a single transaction for the purpose of this section and the operator shall set out in the gaming premises' internal control document the 24-hour period that shall be applicable to the gaming premises;

d) For the purpose of recording transactions over a 24-hour period, an operator shall begin monitoring and recording the transactions of any patron who has received from or provided to the operator the following amounts, and shall continue such monitoring and recording until the end of the 24-hour period:
   i. $3,000 for casino operators.

e) A record generated in accordance with this section shall be disclosed to the Financial Intelligence Agency and any operator who does not disclose in accordance with this section shall be liable to disciplinary action.

A.7 Anti-Money Laundering/Anti-Terrorist Financing (AML/ATF)

A.7.1 AML/ATF Audit.

The operator used in relation to AML/ATF matters shall ensure that its AML/ATF compliance policy is reviewed and an opinion prepared by an independent entity approved by the Commission prior to the opening of the gaming premises and at such intervals as the Commission may by written direction require, in order to assess and measure its continued ability to detect and mitigate existing and emerging risks posed by gaming for the potential of money laundering and terrorist financing, including the controls within this section.

a) The review shall include, but shall not be limited to:
   i. Customer due diligence;
   ii. Transaction monitoring;
   iii. Record keeping;
   iv. Training;
   v. Adherence to reporting requirements;
   vi. Compliance with AML/ATF rules and regulations generally; and
   vii. Compliance with industry good practice.

b) The opinion shall address the compliance of the AML/ATF compliance policy with the requirements of these Regulations and any other provisions of law relating to AML/ ATF.

A.7.2 AML/ATF Compliance Policy.

The internal control document shall set out the comprehensive and robust AML/ATF compliance policy, that is risk-based and will ensure compliance with all the operators' AML/ATF obligations. At a minimum, the AML/ATF compliance policy shall provide for:

a) Procedures for using all reasonably available information to determine:

i. The full name, date of birth, and residential address, and verification of the same, of a patron of the gaming premises, when required by the Commission or any other law enforcement agency to provide such information; and

ii. Whether a suspicious activity report needs to be filed.

b) Appropriate, ongoing training of gaming premises personnel in AML/ATF matters, including:

i. Identification of unusual or suspicious transactions;

ii. A clear reporting line and escalation path; and

iii. The creation and maintenance of any records required.

c) Assigning the compliance officer and their responsibilities in relation to AML/ATF matters including reporting unusual or suspicious transactions and a clear procedure for the review and implementation of any compliance officer recommendations or reports;

d) Monitoring patron accounts for opening and closing in short time frames and for deposits and withdrawals without associated gaming;

e) Ensuring that aggregate transactions over a defined period may require further due diligence checks and may be reportable to the relevant organization(s) if they exceed the threshold prescribed by the Commission;

f) Internal testing for compliance with the requirements of the gaming and AML/ATF legislation;

g) Integrating and sharing data as appropriate and feasible among:

i. Different parts of the gaming premises and integrated resort;

ii. Any other operators;

iii. Other entities providing gaming, betting or lottery services; and

iv. Affiliates in other jurisdictions.

h) Consideration of all remuneration and employee incentive policies and structures to ensure that no person is rewarded as a result of failing to comply with the AML/ATF compliance policy;

i) Procedures to ensure that high risk or politically exposed persons are identified so that appropriate sign-off is obtained for transactions involving those persons;

j) Procedures to implement such measures as are necessary to assist any law enforcement or regulatory authorities in Bermuda with any investigations or enabling those authorities to freeze or seize assets where permitted by law;

k) The use of any automated data processing systems to monitor the variety, frequency and volume of transactions to aid in assuring compliance; and

l) Periodic independent tests for compliance with a scope and frequency as required by the Commission. Logs of all tests shall be maintained.

A.7.3 AML/ATF Risk Assessment.

The operator shall conduct a risk assessment to identify any areas of its operations at risk for money laundering and terrorist financing and the AML/ATF compliance policy shall specify the measures to address those risks. The risk assessment shall cover, but not be limited to, the risks involving:

a) Patrons generally, which may include whether a patron:
   i. Has sources of wealth or income commensurate with his gaming activity;
   ii. Has provided personal, financial or business information that can be readily verified;
   iii. Has fiduciary obligations that may create a risk of misappropriation of funds;
   iv. Is associated with individuals or entities known to be connected to the illicit generation of funds or the laundering of such funds;
   v. Has been made bankrupt;
   vi. Has a prior history of criminal or dishonest conduct; or
   vii. Is a politically exposed person;

b) Casino gaming, and eGaming generally;

c) Products and services offered by or on behalf of the operator;

d) Employees in the proper performance of their functions and duties and as a voluntary or involuntary part of any AML/ATF scheme;

e) The use of foreign holding accounts where funds are held in a foreign jurisdiction for use in a gaming premises in Bermuda;

f) The use of third-party marketing agents and junkets;

g) The ownership structures and integrity of intermediaries and associated businesses such as junket promoters, agents, gaming manufacturers, financial service providers;

h) Criminal activities and proceeds of crime generated domestically as well as generated abroad but laundered domestically;

i) Financial services offered by the operator or by an intermediary; and

j) The use of cashless terminals that accept cash.

A.7.4 AML/ATF Internal Review.

The operator shall review its risk assessment and compliance policy at regular intervals and in light of any changes of circumstances, including the introduction of new products or technology, new methods of payment by patrons, changes in the patron demographic or any material changes, and in any event at least annually. The operator shall:

a) Consider such amendments to the AML/ATF compliance policy as may be recommended and make such amendments as may be required by those persons carrying out the review, the Commission, or the independent entity providing the opinion;

b) Keep a record that demonstrates that:

   i. It takes all relevant risk factors into account when determining the level of AML/ATF risk; and

   ii. AML/ATF risk assessments are not unduly influenced or compromised by the potential profitability of new or existing patron relationships.

c) Seek, through its AML/ATF compliance policy and otherwise, to create to the greatest extent possible a culture where significant importance is attached to AML/ATF;

d) Seek to utilise the Cashless Wagering System or patron account information to aid in complying with the provisions of these Regulations;

e) Ensure that adequate resources are allocated to ensure compliance with all AML/ATF requirements; and

f) Ensure that any employees in a jurisdiction other than Bermuda comply with all record keeping and recording requirements set out in the Acts or Regulations.

A.7.5 AML/ATF Compliance Officer.

The operator shall ensure that it has at all times a compliance officer. The compliance officer shall:

a) Be adequately trained to carry out the role;

b) Fully understands the relevant AML/ATF requirements;

c) Be available to other employees to consult on AML/ATF related issues as they arise;

d) Be fully knowledgeable as to the operator's products, services, customer base and particular AML/ATF risk areas;

e) Have appropriate authority and resources to implement the operator's AML/ ATF policies; and

f) Be responsible for ensuring that training is provided at a minimum to the following general categories of employees:

   i. Those engaged in the gaming operation;

   ii. All employees with cash or credit handling responsibilities;

   iii. Surveillance employees;

   iv. Employees in the accounts department;

   v. Senior gaming management; and

   vi. Employees responsible for marketing or hosting high value patrons.

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 terminals. 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 patron identification.

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

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

Cashless Terminal – An electronic device that converts communications from the Cashless Wagering System into a human interpretable form and converts human decisions into communication format understood by the Cashless Wagering System. Cashless terminals refer to kiosks, gaming machines and any other equipment used for wagering at a gaming premises.

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

Cashless Wagering System – An electronic system that allows an operator to offer its patrons a way of placing stakes and receiving winnings, without using cash or chips, by means of direct debiting and crediting of the patron account.

CEP, *Cashable Electronic Promotion* – Cashable Incentive credits electronically transferred to/from a cashless terminal from/to a patron 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 patron 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 patron 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 terminal through a Cashless Wagering System.

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

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 Machine – means any device, whether wholly or partly mechanically or electronically operated, that is so designed that— it may be used for the purpose of playing a game of chance or a game of mixed chance and skill; and as a result of making a wager on the device, winnings may become payable.

Gaming Premises – A casino premises.

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

Incentive Award – An award that is not described in the paytable of a game, that is based upon predefined patron activity criteria established by the parameters of the Cashless Wagering System that are tied to a specific patron 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.

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 patron 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 credits electronically transferred to/from a cashless terminal from/to a patron account.

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

Operator – is a casino operator that operates a Cashless Wagering System, using both the technological capabilities of the Cashless Wagering 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.

Patron Account (aka “Wagering Account” / “Cashless Account”) **–** An account to the credit of a patron for purposes of gaming whether it is a credit account, a cheque cashing account, a deposit account or any other account opened by or on behalf of a patron with an operator.

Patron Account Transfer (aka “Wagering Account Transfer” / “Cashless Account Transfer”) – An electronic transfer of funds between a Cashless Wagering System's patron account and a cashless terminal.

Patron Data – Sensitive information regarding a patron 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.

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

Patron Loyalty Program – A program that provides incentive awards for patrons based on the volume of play or revenue received from a patron.

Peripheral – An internal or external device connected to a cashless terminal that supports credit acceptance, credit issuance, patron 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.

Prepaid Access Instrument – A card, code, electronic serial number, mobile identification number, personal identification number or similar device used in conjunction with a Cashless Wagering System that allows patron 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.

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, patron 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 terminal with an external system, supporting protocol conversion between the machine and the system.

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

Tilt – An error in cashless terminal 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 Wagering 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 patron's device and the cashless terminal which is used for credit insertion and redemption.

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