INDEPENDENT
GAMBLING CONTROL
OFFICE

TGS3

Technical Gaming Standard for On-Line Monitoring and Control Systems and Validation Systems in Casinos

Version 2.0 – April 13, 2026

BRITISH COLUMBIA

Table of Contents

1. Overview

1.1 Introduction

1.1.1 Purpose

This Technical Gaming Standard (standard) outlines requirements for on-line monitoring and control systems (MCSs) and validation systems used in B.C. casinos, including requirements:

a) for testing systems;
b) that systems must meet to receive approval from the Independent Gambling Control Office (IGCO) for use in a lottery scheme; and
c) for the operation of a lottery scheme using an approved system.

1.1.2 Changes from Previous Version of this Standard

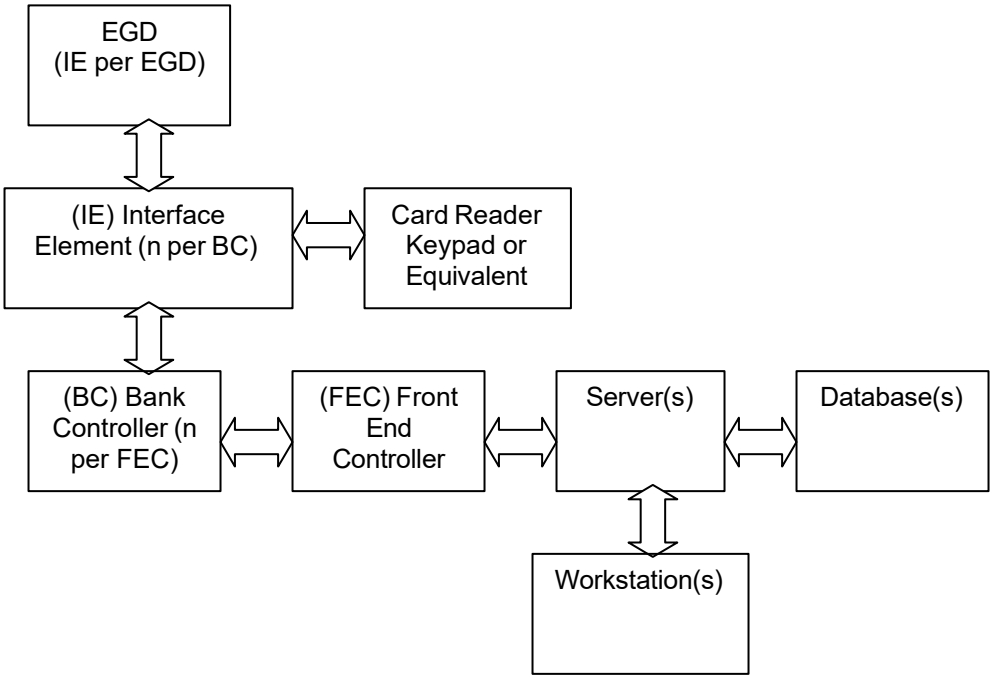
This standard replaces version 1.3 of B.C.'s Technical Gaming Standard for On-Line Monitoring and Control Systems (MCSs) and Validation Systems in Gaming Venues. Changes from the previous version of the standard include:

a) Updates required to align with the new B.C. *Gaming Control Act* and regulations that came into force on April 13, 2026;
b) Updates to reflect the renaming of the Gaming Policy and Enforcement Branch (GPEB) as the IGCO;
c) Deletion of requirements relating to the content of submissions to Independent Testing Laboratories (ITLs). The IGCO expects that ITLs will work with the BC Lottery Corporation (BCLC) and registered gaming suppliers to ensure all relevant information is provided to enable adequate testing;
d) Edits to improve the clarity and consistency of language used within the standard; and
e) Elimination of requirements that were clearly outdated based on current technology.

1.1.3 MCS Defined

An MCS is a game management system that continuously monitors an electronic gaming device (EGD) via a defined communication protocol by either a dedicated line, dial-up system, or other secure transmission method such as Wireless Ethernet Communications. An MCS is primarily tasked to provide logging, searching, and reporting of gaming significant events, collection of individual device financial and meter data, reconciliation of meter data against hard and soft counts, and systems security.

The block diagram below is a visual depiction of a generic MCS and is not intended to mandate any particular component or system topology providing adequate / equivalent functionality is maintained. The terms used to identify individual components in the diagram are used throughout this standard.



1.1.4 Application of this Standard

This standard applies to all components referenced in the diagram above, other than EGDs. The requirements for EGDs are outlined in TGS1 – Technical Gaming Standard for Gaming Devices in Casinos. This standard only concerns communications from the EGD to the MCS, and not in the reverse order, with the exception of the Ticket Validation System requirements that are incorporated within Chapter 4.

This standard only includes MCS requirements necessary to achieve IGCO approval when interfaced to coin/bill-drop and ticket-drop EGDs, for the purpose of communicating mandatory security events and electronic meters. This infers that all relevant monetary transactions at the EGD level are handled through:

a) Credit Issuance:
   i. Coins or tokens accepted via approved coin acceptors;
   ii. Currency notes (Bills) accepted via approved bill acceptors; and
   iii. Approved Tickets (Items) accepted via approved bill/ticket acceptors.
b) Credit Redemption:
   i. Coins or tokens paid by approved hoppers;
   ii. Handpays; and
   iii. Tickets (Items) paid by approved ticket printers.

This standard does not include MCS requirements for any other form of monetary transaction. This standard also does not govern advanced bi-directional communication protocols (i.e. EFT, Bonusing, Promotional, system progressive controllers, features that utilize a Random Number Generator (RNG), etc.) that support credit transfer between EGD and MCS. This standard only supports one-way communication of events originated at the EGD level to the MCS with the exception of the Ticket Validation System Requirements that are incorporated within Chapter 4.

1.1.5 Other Technical Gaming Standards That May Apply

The following standards may apply to other components of an EGD system:

a) TGS1 – Technical Gaming Standard for Gaming Devices in Casinos;
b) TGS2 – Technical Gaming Standards for Progressive Gaming Devices in Casinos; and/or
c) TGS4 – Technical Gaming Standards for Electronic Bingo Systems in Gaming Venues.

1.1.6 Conflict with Legislation or Regulation

In the event of a conflict between this standard and the provisions of the *Gaming Control Act*, its regulations, or any other applicable legislation or regulation, the legislation or regulation applies.

2. System Component Requirements

2.1 Interface Element Requirements

2.1.1 General Statement

Each EGD installed in the gaming venue must have a device or facility (interface element) installed inside a secure area of the EGD, that provides for communication between the EGD and an external Data Collector.

2.1.2 Metering Requirements

If not directly communicating EGD meters, the interface element must maintain separate electronic meters, of sufficient length, to preclude the loss of information from meter rollovers, or a means to identify multiple rollovers, as provided for in the connected EGD. These electronic meters must be capable of being reviewed on demand, at the interface element level via an authorized access method (see also Section 3.3 Meters).

2.1.3 Battery Backup Requirements

The interface element must retain the required information after a power loss for a period determined by BCLC and the IGCO. If this data is stored in volatile RAM, a battery backup must be installed within the interface element (see also Section 3.3 Meters).

2.1.4 Information Buffering and Integrity Checking

If unable to communicate the required information to the MCS, the interface element must provide a means to preserve all mandatory meter and significant event information until such time as it can be communicated to the MCS (see also Section 3.2 Significant Events and Section 3.3 Meters). EGD operation may continue until critical data will be overwritten and lost. There must be a method to check for corruption of the above data storage locations.

2.1.5 Address Requirements

The interface element must allow for the association of a unique identification number to be used in conjunction with an EGD file on the MCS. This identification number will be used by the MCS to track all the mandatory information of the associated EGD. Additionally, the MCS must not allow for duplicate EGD file entry of this identification number.

2.1.6 Configuration Access Requirements

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

2.2 Front End Controller and Data Collector Requirements

2.2.1 General Statement

An MCS may possess a Front End Processor (FEP) that gathers and relays all data from the connected Data Collectors to the associated database(s). The Data Collectors, in turn, collect all data from connected EGDs. Communication between components must be via an approved method and at minimum conform to the communication protocol requirements stated in Section 3.1 Communication Protocol. If the FEP maintains buffered/logging information, then a means must exist which prevents the loss of critical information contained herein.

2.3 Server and Database Requirements

2.3.1 General Statement

An MCS will possess a Server(s), networked system or distributed systems that direct overall operation and an associated database(s) that stores all entered and collected system information.

2.3.2 System Clock

An MCS must maintain an internal clock that reflects the current time (24hr format - which is understood by the local date/time format) and date that must be used to provide for the following:

a) Time stamping of significant events;
b) Reference clock for reporting; and
c) Time stamping of configuration changes.

2.3.3 Synchronization Feature

If multiple clocks are supported, an MCS must have a facility whereby it is able to update those clocks in MCS components, whereby conflicting information could occur.

2.3.4 Database Access

An MCS must not have a built-in facility whereby an unauthorized individual can bypass system auditing to modify the database directly. Gaming services providers must maintain secure access control.

2.4 Workstation Requirements

2.4.1 Jackpot/Fill Functionality

An MCS must have an application or facility that captures and processes every hand pay message from each EGD. Hand pay messages must be created for single wins (jackpots), progressive jackpots and accumulated credit cash outs (cancelled credits), which result in hand pays. A Fill (deposit of a predetermined or otherwise properly authorized, token amount in an EGD's hopper) is normally initiated from a hopper empty message while a Credit (removal of excess tokens from an EGD) is normally user initiated. An allowable exception to fill initiation would be where the system provides preventative or maintenance fill functionality, in which the transaction may be initiated by the system or an authorized user. Once captured, there must be adequate access controls to allow for

authorization, alteration, or deletion of any of the values prior to payment or execution.

2.4.2 Large Cash Transactions Reporting (LCTR) Threshold

All winners of jackpots in excess of $9,999.99, in gaming venues in British Columbia, are required under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act/Regulations to complete a Large Cash Transaction and Foreign Exchange Record (LCTR) at the time of the win.

2.4.3 Jackpot/Fill Slip Information

The following information is required for all slips generated with some/all fields to be completed by the MCS:

a) Type of slip;
b) Numeric Slip identifier (which increments per event);
c) Date and Time;
d) EGD number;
e) Denomination;
f) Amount of Fill;
g) Amounts of Jackpot, Accumulated Credit, and Additional Pay;
h) Additional Payout, if applicable;
i) Amount to Patron;
j) Total coins played and game outcome of award;
k) Soft meter readings; and
l) Relevant signatures as required by BCLC Internal Control procedures.

Note: Items 'e' and 'f,' apply to fill slips and items 'g' through 'l' apply to jackpot slips.

2.4.4 Surveillance/Security Functionality

An MCS must provide an interrogation program that enables on-line comprehensive searching of the significant event log for the present and for the previous 14 days through archived data or restoration from backup where maintaining such data on a live database is deemed inappropriate. The interrogation program must have the ability to perform a search based at least on the following:

a) Date and Time range;
b) Unique interface element/EGD identification number; and
c) Significant event number/identifier.

2.4.5 EGD Management Functionality

An MCS must have a master "EGD file" which is a database of every EGD in operation including, at minimum, the following information for each entry. If the MCS retrieves any of these parameters directly from the EGD, sufficient controls must be in place to ensure accuracy of the information.

a) Unique interface element/location identification number;
b) EGD identification number as assigned by the gaming venue;
c) Denomination of the EGD;
d) Theoretical hold of the EGD; and
e) Control program(s) within the EGD.

2.4.6 Accounting Functionality

An MCS must have an application or facility that allows controlled access to all accounting (financial) information and is able to create all mandatory reports in Section 3.4 Reporting Requirements, as well as all Internal Control required reports, if specified.

2.4.7 Exclusions

Generally, any system (component) not specified in this standard that impacts revenue reporting must be tested and approved by the IGCO. For example, a Standalone Player Tracking System does not need to be tested and approved unless its function includes embedded feature(s) that affect revenue. However, it may be tested for operation and version control if an integrated feature of an MCS.

3. System Requirements

3.1 Communication Protocol

3.1.1 General Statement

An MCS must support a defined communication protocol(s) that provides for the following:

a) All critical data communication must be protocol based and/or incorporate an error detection and correction scheme to ensure an accuracy of 99% or better of messages received; and
b) All critical data communication that may affect revenue and is unsecured either in transmission or implementation must employ encryption. The encryption algorithm must employ variable keys, or similar methodology to preserve secure communication.

Note: This standard does not preclude the use of radio frequency technology in any of the system components, but should Wi-Fi technology be used, then a document must be provided that details how the security concerns are to be addressed.

3.2 Significant Events

3.2.1 General Statement

Significant events are generated by an EGD and sent via the interface element to the MCS utilizing an approved communication protocol. Each event must be stored in a database(s) which includes the following:

a) Date and time when the event occurred;
b) Identity of the EGD that generated the event;
c) A unique number/code that defines the event; and
d) A brief text that describes the event in English.

3.2.2 Standard Events

The following significant events must be collected from the EGD and transmitted to the system for storage:

a) Power Resets or power failure;
b) Hand pay Conditions (amount needs to be sent to the system);
    i. EGD Jackpot (An award in excess of the single win limit of the EGD);
    ii. Cancelled Credit Hand pay; and
    iii. Progressive Jackpot (As per Jackpot above);
c) Door Openings (any external door on the EGD that accesses a critical area) (Note: Door switches (discrete inputs to the interface element) are acceptable if their operation does not result in redundant or confusing messaging);
d) Coin or Token-In Errors ('I' and 'ii' should be sent as unique messages if supported in protocol);

    i. Coin or Token jams; and
    ii. Reverse Coins or tokens-in;
e) Bill (Item) Acceptor Errors ('i' and 'ii' should be sent as unique messages if supported in protocol);
    i. Stacker Full (if supported); and
    ii. Bill (Item) jam;
f) EGD Low RAM Battery Error;
g) Reel Spin Errors (if applicable with individual reel number identified);
h) Coin or Token-Out Errors ('i' and 'ii' should be sent as unique messages if supported in the protocol);
    i. Hopper jams;
    ii. Hopper runaways or extra coins paid out; and
    iii. Hopper empties (must be sent as a unique message);
i) Printer Errors (if printer supported);
    i. Printer Empty/Paper Low; and
    ii. Printer Disconnect/Failure.

3.2.3 Priority Events

The following significant events must be conveyed to the MCS where a mechanism must exist for timely notification:

a) Loss of Communication with Interface element;
b) Loss of Communication with EGD;
c) Memory corruption of the Interface element, if storing critical information; and
d) RAM corruption of the EGD.

3.3 Meters

3.3.1 General Statement

Metering information is generated on an EGD and collected by the interface element and sent to the MCS via a communication protocol. This information may be either read directly from the EGD or relayed using a delta function.

3.3.2 Required Meters

The following metering information must be communicated from the EGD:

a) Total In (credits-in);
b) Total Out (credits-out);
c) Total Dropped (coins-dropped or total value of all coins, bills and tickets dropped);
d) Hand Paid (hand-pays);
e) Cancelled Credits (if supported on EGD);
f) Bills In (total monetary value of all bills accepted);
g) Individual Bill Meters (total number of each bill accepted per denomination);
h) Games-Played;
i) Cabinet Door (instance meter which may be based on MCS count of this event);
j) Drop Door(s) (instance meter which may be based on MCS count of this event);
k) Ticket In (total monetary value of all tickets accepted); and
l) Ticket Out (total monetary value of all tickets produced).

Note: Please refer to TGS1 – Technical Gaming Standard for Gaming Devices in Casinos for standards for the electronic accounting meters that must be maintained by the EGD. While these electronic accounting meters should be communicated directly from the EGD to the MCS, it is acceptable to use secondary MCS calculations where appropriate.

3.3.3 Clearing Meters

An interface element must not have a mechanism whereby an unauthorized user can cause the loss of stored accounting meter information (see also Section 2.1.4 Information Buffering and Integrity Checking).

Note: This is typically only valid for systems that utilize a delta metering scheme.

3.4 Reporting Requirements

3.4.1 General Statement

Significant event and metering information is stored on the MCS in a database and accounting reports are subsequently generated by querying the stored information.

3.4.2 Required Reports

Reports will be generated on a schedule determined by BCLC (to be approved by the IGCO), which typically consists of daily, monthly, yearly period, and life to date reports generated from stored database information. These reports at minimum will consist of the following:

a) Net Win/Revenue Report for each EGD;
b) Drop Comparison Reports for each medium dropped (examples = coins, bills) with dollar and percent variances for each medium and aggregate for each type;
c) Metered vs. Actual Jackpot comparison Report with the dollar and percent variances for each and aggregate;
d) Theoretical Hold vs. Actual Hold comparison with variances; and
e) Significant Event Log for each EGD.

Note: It is acceptable to combine reporting data where appropriate (e.g., revenue, theoretical/actual comparison)

Note: For additional revenue reporting requirements when ticket drop EGDs are interfaced, see Chapter 4 Ticket Validation System Requirements.

Note: If any advanced bi-directional communication protocol is supported, the revenue reporting will change.

3.5 Security Requirements

3.5.1 Access Control

An MCS must support either a hierarchical role structure whereby user and password define program or individual menu item access or logon program/device security based strictly on user and password or PIN. In addition, an MCS must not permit the alteration of any significant log information communicated from the EGD. Additionally, there should be a provision for system administrator notification and user lockout or audit trail entry, after a set number of unsuccessful login attempts.

3.5.2 Data Alteration

An MCS must not permit the alteration of any accounting or significant event log information that was properly communicated from the EGD without supervised access controls. In the event financial data is changed, an audit log must be capable of being produced to document:

a) Data element altered;
b) Data element value prior to alteration;
c) Data element value after alteration;
d) Time and Date of alteration; and
e) Personnel that performed alteration (user login).

3.6 Additional System Features

3.6.1 EGD Program Verification Requirements

If supported, an MCS may provide this redundant functionality to check EGD game software. Although the overhead involved can potentially impede EGD and MCS operation, the following information must be reviewed for validity prior to implementation:

a) Software signature algorithm(s); and
b) Data communications error check algorithm(s).

3.6.2 Verification Algorithm Timing

Verification may be user initiated or triggered by specific significant event(s) on the EGD. To ensure complete coverage verification must be performed after each of the following events:

a) EGD Power Up; and
b) New EGD installed.

3.6.3 FLASH Download Requirements

If supported, an MCS may utilize FLASH technology to update interface element software if all of the following requirements are met:

a) FLASH Download functionality must be, at a minimum, password protected, and should be at a supervisor level. The MCS can continue to locate and verify versions currently running but it cannot load code that is not currently running on the system without user intervention;
b) A non-alterable audit log must record the time/date of a FLASH download and some provision must be made to associate this log with, which version(s) of code was downloaded, and the user who initiated the download. A separate FLASH Audit Log Report would be ideal; and
c) All modifications to the download executable or flash file(s) must be submitted to BCLC for evaluation, and approval by the IGCO. At this time, BCLC and/or the ITL will perform a FLASH download to the system existing at the BCLC testing facility and verify operation. BCLC will then assign signatures to any relevant executable code and flash file(s) that can be verified by a BCLC or IGCO representative in the field.

Note: The above refers to loading of new system executable code only. Other program parameters may be updated as long as the process is securely controlled and subject to audit.

3.6.4 Remote Access Requirements

If approved by BCLC and the IGCO, an MCS may utilize password controlled remote access to an MCS as long as the following requirements are met:

a) Remote Access User Activity log is maintained depicting logon name, time/date, duration, activity while logged in;
b) No unauthorized remote user administration functionality (adding users, changing permissions, etc.);
c) No unauthorized access to database other than information retrieval using existing functions;
d) No unauthorized access to operating system; and
e) If remote access is to be continuous basis then a network filter (firewall) must be installed to protect access.

Note: BCLC may allow the MCS manufacturer, as needed, to remotely access the MCS and its associated components for the purpose of product and user support. The IGCO must grant approval for any such activities before BCLC may proceed.

3.7 Backups and Recovery

3.7.1 General Statement

An MCS must have sufficient redundancy and modularity so that if any single component or part of a component fails, gaming can continue. There must be redundant copies of each log file or system database or both on the MCS with open support for backups and restoration.

3.7.2 Recovery Requirements

In the event of a catastrophic failure when an MCS cannot be restarted in any other way, it must be possible to reload the system from the last viable backup point and fully recover the contents of that backup, recommended to consist of at least the following information:

a) Significant events;
b) Accounting information;
c) Auditing information; and
d) Specific site information such as slot file, employee file, progressive set-up, etc.

4. Ticket Validation System Requirements

4.1 Introduction

4.1.1 General Statement

A ticket validation system may be entirely integrated into an MCS or exist as an entirely separate entity. Ticket validation systems are generally classified into two types: bi-directional ticket systems that allow for EGD ticket insertion and ticket out only systems that do not allow this. This section primarily concerns bi-directional ticket systems. Where ticket out only systems are utilized, some of the following may not apply.

4.1.2 Payment by Ticket Printer

Payment by ticket printer as a method of credit redemption on an EGD is only permissible when the EGD is linked to an approved validation system or MCS that allows validation of the printed ticket. Validation information must come from the validation system or MCS using a secure communication protocol.

4.2 Ticket Information

4.2.1 General Statement

A ticket must contain the following printed information, at a minimum:

a) Casino Name/Site Identifier;
b) Machine Number (or Cashier/Change Booth location number, if ticket creation, outside the EGD, is supported);
c) Date and Time (24hr format which is understood by the local date/time format);
d) Alpha and numeric dollar amount of the ticket;
e) Ticket sequence number;
f) Validation number;
g) Bar code or any machine readable code representing the Validation number;
h) Type of transaction or other method of differentiating ticket types (assuming multiple ticket types are available); and
i) Indication of an expiration period from date of issue, or date and time the ticket will expire (24hr format which is understood by the local date/time format).

Note: Some of this information may be contained in the validation number.

4.2.2 Ticket Types

If EGD ticket generation is to be supported while not connected to the validation system, a ticket system must generate two different types of tickets at minimum. On-line and off-line types are denoted respectively by ticket generation either when the validation system and EGD are properly communicating or the validation system and EGD are not communicating properly. When a patron cashes out of an EGD that has lost communication with the validation system, the EGD must lock up and, after reset, may print an off-line ticket or handpay receipt. The ticket or handpay receipt must be visually distinct from an on-line ticket either in format or content while still maintaining all information required.

4.3 Ticket Issue and Redemption

4.3.1 Ticket Issuance

A ticket can be generated at an EGD through an internal document printer, at a player's request, by redeeming all credits. Tickets that reflect partial credits may be issued automatically from an EGD. Additionally, cashier/change booth issuance is allowed if supported by the validation system.

4.3.2 Online Ticket Redemption

Tickets may be inserted in any EGD participating in the validation system provided that no credits are issued to the EGD prior to confirmation of ticket validity. The customer may also redeem a ticket at a cashier/change booth or other approved validation terminal.

4.3.3 Cashier/Change Booth Operation

All validation terminals must be user and password controlled. Once presented for redemption, the cashier must:

a) Scan the bar code via an optical reader or equivalent;
b) Input the ticket validation number manually; or
c) Print a validation receipt, after the ticket is electronically validated.

4.3.4 Validation Receipt Information

The validation receipt, at a minimum, must contain the following printed information:

a) Machine number;
b) Validation number;
c) Date and Time paid;
d) Amount; and
e) Cashier/Change Booth identifier.

4.3.5 Invalid Ticket Notification

A validation system or MCS must have the ability to identify these occurrences and notify the cashier that one of the following conditions exists:

a) Ticket cannot be found on file (stale date, forgery, etc.);
b) Ticket has already been paid; or
c) Amount of ticket differs from amount on file (requirement can be met by display of ticket amount for confirmation by cashier during the redemption process).

4.3.6 Offline Ticket Redemption

If an on-line data system temporarily goes down and validation information cannot be sent to the validation system or MCS, an alternate method of payment must be provided either by the validation system possessing unique features, (e.g., validity checking of ticket information in conjunction with a local database storage), to identify duplicate tickets and prevent fraud by reprinting and redeeming a ticket that was previously issued by the EGD; or use of an approved alternative method that will accomplish the same.

4.4 Reports

4.4.1 Reporting Requirements

The following reports must be generated at a minimum and reconciled with all validated/redeemed tickets:

a) Ticket Issuance Report;
b) Ticket Redemption Report;
c) Ticket Liability Report;
d) Ticket Drop Variance Report;
e) Transaction Detail Report must be available from the validation system that shows all tickets generated by an EGD and all tickets redeemed by the validation terminal or other EGD; and
f) Cashier Report to detail individual and sum of tickets paid by cashier/change booth or validation unit.

Note: The requirements for 'b' & 'd' are waived where two-part tickets exist for the EGD where the first part is dispensed as an original ticket to the patron and the second part remains attached to the printer

mechanism as a copy (on a continuous roll) in the EGD.

4.5 Security

4.5.1 Database and Validation Component Security

Once the validation information is stored in the database, the data may not be altered in any way. The validation system database must be encrypted or password-protected and must possess a non-alterable user audit trail to prevent unauthorized access. Further, the normal operation of any device that holds ticket information must not have any options or method that may compromise ticket information. Any device that holds ticket information in its memory must not allow removal of the information unless it has first transferred that information to the database or other secured component(s) of the validation system.

5. System Environmental and Safety Requirements

5.1 Introduction

5.1.1 General Statement

This section outlines the environmental and safety requirements for all system components.

5.2 Hardware and Player Safety

5.2.1 General Statement

Electrical and mechanical parts and design principals of the EGD must not subject a player to any physical hazards.

5.3 Environmental Effects on System Integrity

5.3.1 Integrity Standard

BCLC and/or the ITL must perform certain tests to determine whether or not outside influences affect game fairness to the player or create cheating opportunities. An on-line system must be able to withstand the following tests, resuming game play without operator intervention:

a) Electro-magnetic Interference. Systems must not create electronic noise that affects the integrity or fairness of the neighbouring associated equipment;
b) Electro-static Interference. Protection against static discharges requires that the system's hardware be earthed in such a way that static discharge energy does not damage or inhibit the normal operation of the electronics or other components within the system. Systems may exhibit temporary disruption when subjected to a significant electro-static discharge greater than human body discharge, but they must exhibit a capacity to recover and complete any interrupted function without loss or corruption of any control or data information associated with the system. The tests must be conducted with a severity level of up to 27KV air discharge;
c) Radio Frequency Interference (RFI). Systems must not divert from normal operation by the application of RFI at a frequency range from 27 to 1000 MHz with a field strength of 3 volts per meter (Note: This requirement may be waived or modified where the mode of communication of the system component being tested is via radio frequency transmission);
d) Magnetic Interference. Systems must not be adversely affected by Magnetic Interference.