
Gaming Policy and Enforcement Branch (GPEB)

TGS3

Technical Gaming Standards for On-Line Monitoring and Control Systems (MCSs) and Validation Systems in Gaming Venues

Technical Standards Document (TSD) Version 1.3



BRITISH COLUMBIA

**Ministry of Public Safety
and Solicitor General**

Gaming Policy and Enforcement Branch

3rd Floor, 910 Government Street
P.O. Box 9202 Stn. Prov. Govt.
Victoria, British Columbia, Canada
V8W 9J1

© Gaming Policy and Enforcement Branch.

All rights reserved. No part of this document may be reprinted, reproduced, stored in a retrieval system or transmitted, in any form or by any means, without prior permission in writing from the Gaming Policy and Enforcement Branch, other than for the internal business use of the British Columbia Lottery Corporation.

Initially published and distributed on January 4, 2006.


 BRITISH COLUMBIA	Technical Standards Document (TSD)	
	Regulatory Body:	GPEB
	Operating Body:	BCLC
	Document Reference:	TGS3
	Document Version:	Version 1.3, January 4, 2006
Gaming Policy and Enforcement Branch (GPEB)		


Table of Contents

1	Overview of TSD	5
1.1	Introduction	5
1.1.1	General Statements I	5
1.1.2	General Statement II	5
1.1.3	MCS Defined	5
1.1.4	Phases of Certification	5
1.2	Acknowledgment of Other TSDs Reviewed	6
1.2.1	General Statement	6
1.3	Graphical Overview	6
1.3.1	General Statement	6
1.4	Purpose of TSD	6
1.4.1	General Statement	6
1.4.2	No Limitation of Technology	7
1.4.3	Scope of TSD	7
1.4.4	Exceptions to TSD	7
1.5	Other TSDs That May Apply	7
1.5.1	General Statement	7
2	Submission Requirements	8
2.1	Introduction	8
2.1.1	General Statement	8
2.1.2	Previous Submission	8
2.2	Prototype (Full Submission) Submissions	8
2.2.1	General Statement	8
2.2.2	Submission Letter Requirements	8
2.3	System Hardware Submission Requirements – Prototype (Full Submission) Certification	9
2.3.1	Presentation of Equipment to BCLC and/or the ATF; Identical Equipment	9
2.3.2	Inventory of Equipment to BCLC and/or the ATF	9
2.3.3	Accompanying Documentation	9
2.4	System Software Submission Requirements – Prototype (Full Submission) Certification	9
2.4.1	General Statement	10
2.5	Software Programming Requirements and Compilation	10
2.5.1	General Statement	10
2.5.2	Source Code Commented	10
2.5.3	Source Code Completeness	10
2.6	Program Identification	10
2.6.1	Software Requirements	10
2.6.2	Firmware Requirements	10
2.7	Submissions of Modifications (Partial Submissions) to a Previously Certified Item	11
2.7.1	General Statement	11
2.7.2	Modification of Hardware	11
2.7.3	Modification of System Software Functions or to Correct Software Error	11
2.7.4	Software Submission -Modification to Existing or Create New System Functionality	11
2.8	System Security Submission Requirements	11
2.8.1	General Statement	11
2.9	Joint Venture Submissions	11
2.9.1	General Statement	12
3	System Component Requirements	12
3.1	Interface element Requirements	12
3.1.1	General Statement	12
3.1.2	Metering Requirements	12



Technical Standards Document (TSD)	
Regulatory Body:	GPEB
Operating Body:	BCLC
Document Reference:	TGS3
Document Version:	Version 1.3, January 4, 2006
Gaming Policy and Enforcement Branch (GPEB)	

- 3.1.3 Battery Backup Requirements 12
- 3.1.4 Information Buffering and Integrity Checking..... 12
- 3.1.5 Address Requirements 12
- 3.1.6 Configuration Access Requirements..... 13
- 3.2 Front End Controller and Data Collector Requirements..... 13
 - 3.2.1 General Statement..... 13
- 3.3 Server and Database Requirements 13
 - 3.3.1 General Statement..... 13
 - 3.3.2 System Clock 13
 - 3.3.3 Synchronization Feature 13
 - 3.3.4 Database Access 13
- 3.4 Workstation Requirements 13
 - 3.4.1 Jackpot/Fill Functionality 13
 - 3.4.2 Large Cash Transactions Reporting (LCTR) Threshold 13
 - 3.4.3 Jackpot/Fill Slip Information 14
 - 3.4.4 Surveillance/Security Functionality 14
 - 3.4.5 EGD Management Functionality 14
 - 3.4.6 Accounting Functionality 14
 - 3.4.7 Exclusions 14
- 4 System Requirements..... 14
 - 4.1 Communication Protocol 15
 - 4.1.1 General Statement..... 15
 - 4.2 Significant Events 15
 - 4.2.1 General Statement..... 15
 - 4.2.2 Standard Events..... 15
 - 4.2.3 Priority Events 16
 - 4.3 Meters..... 16
 - 4.3.1 General Statement..... 16
 - 4.3.2 Required Meters..... 16
 - 4.3.3 Clearing Meters..... 16
 - 4.4 Reporting Requirements..... 16
 - 4.4.1 General Statement..... 16
 - 4.4.2 Required Reports 16
 - 4.5 Security Requirements 17
 - 4.5.1 Access Control 17
 - 4.5.2 Data Alteration 17
 - 4.6 Additional System Features..... 17
 - 4.6.1 EGD Program Verification Requirements 17
 - 4.6.2 Verification Algorithm Timing 17
 - 4.6.3 FLASH Download Requirements 17
 - 4.6.4 Remote Access Requirements 18
 - 4.7 Backups and Recovery..... 18
 - 4.7.1 General Statement..... 18
 - 4.7.2 Recovery Requirements 18
- 5 Ticket Validation System Requirements 18
 - 5.1 Introduction 18
 - 5.1.1 General Statement..... 18
 - 5.1.2 Payment by Ticket Printer 19
 - 5.2 Ticket Information 19
 - 5.2.1 General Statement..... 19
 - 5.2.2 Ticket Types..... 19
 - 5.3 Ticket Issue and Redemption 19

 BRITISH COLUMBIA	Technical Standards Document (TSD)	
	Regulatory Body:	GPEB
	Operating Body:	BCLC
	Document Reference:	TGS3
	Document Version:	Version 1.3, January 4, 2006
Gaming Policy and Enforcement Branch (GPEB)		

5.3.1	Ticket Issuance	19
5.3.2	Online Ticket Redemption.....	19
5.3.3	Cashier/Change Booth Operation.....	19
5.3.4	Validation Receipt Information	20
5.3.5	Invalid Ticket Notification	20
5.3.6	Offline Ticket Redemption.....	20
5.3.7	Wireless Hand-held Ticket Redemption.....	20
5.4	Reports	20
5.4.1	Reporting Requirements	20
5.5	Security.....	20
5.5.1	Database and Validation Component Security	20
6	System Environmental and Safety Requirements	21
6.1	Introduction	21
6.1.1	General Statement.....	21
6.2	Hardware and Player Safety.....	21
6.2.1	General Statement.....	21
6.3	Environmental Effects on System Integrity.....	21
6.3.1	Integrity Standard.....	21
7	Systems using Wireless Networks	22
7.1	Introduction.....	22
7.1.1	General Statement.....	22
7.2	Wireless Ethernet Communications	22
7.2.1	General Statement.....	22
7.3	Security Considerations for WLAN used with a Wired LAN	22
7.3.1	General Statement.....	22

1 Overview of TSD

1.1 Introduction

1.1.1 General Statements I

The General Statements are as follows:

- a) Before being permitted to operate in the live environment, all On-Line Monitoring and Control Systems (MCSs) and Validation Systems used in the Province of British Columbia must be tested to the applicable requirements set forth in this Technical Standards Document (TSD).
- b) The British Columbia Lottery Corporation (BCLC) may select an appropriate Accredited Testing Facility (ATF), or other equivalent body, to perform this testing; however, BCLC's selection requires approval from the Gaming Policy and Enforcement Branch (GPEB).
- c) The appointed testing body must provide their evaluation results to BCLC, who in turn must provide these evaluation results to GPEB for review, and where required, subsequent discussion.
- d) Although the appointed testing body may recommend the approval of any MCSs or Validation Systems for used in the Province of British Columbia, the ultimate authority to approve MCSs and Validation Systems rests solely with GPEB. Only GPEB can issue a Certificate of Technical Integrity under **Section 75 of the Gaming Control Act of British Columbia**.

Note: An "On-Line Monitoring and Control System (MCS) or Validation System" does NOT include, for purposes of this TSD, ancillary electronic equipment used in the conduct of Table Games.

1.1.2 General Statement II

It is the policy of GPEB, in consultation with BCLC, to update this TSD at minimum once annually, to reflect any changes in technology, testing methods, or known cheating methods.

Note: GPEB reserves the right to modify (or selectively apply) the requirements set forth in this TSD as deemed necessary to ensure the integrity of gaming in the Province of British Columbia.

1.1.3 MCS Defined

An MCS is a game management system that continuously monitors each 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 outlined in **Section 4** of this TSD.

1.1.4 Phases of Certification

GPEB approval of an MCS or Validation System may be acquired in two phases:

- a) Initial laboratory testing, where BCLC and/or the ATF, will test the integrity of the system in conjunction with EGDs, in a laboratory setting with the equipment assembled; and
- b) On-site verification where the communications and set up are tested on the gaming venue floor prior to implementation.
- c) Should a wireless network solution be adopted (refer to **Section 7** for further information) then an independent network security auditing company (or qualified ATF) may be used to review the installation and security procedures. In addition, it may be recommended that the system is periodically reviewed by the security auditing company (or qualified ATF) after implementation.

1.2 Acknowledgment of Other TSDs Reviewed

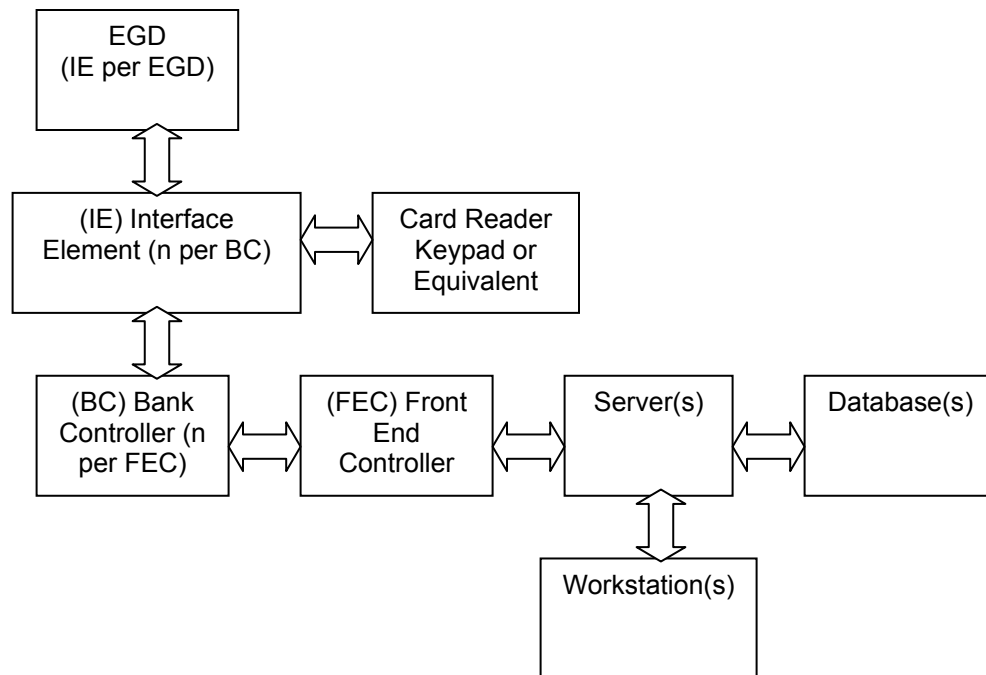
1.2.1 General Statement

This TSD has been developed by reviewing and using portions of the Gaming Laboratories International (GLI) TSD named 'GLI-13'.

1.3 Graphical Overview

1.3.1 General Statement

The purpose of this section is to lend 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 throughout this TSD will be represented in a block diagram format to clarify individual components.



*In the illustration above, this standard applies to all components referenced other than the EGDs. The requirements for the EGDs are defined in TGS1 – Technical Gaming Standards for Electronic Gaming Devices (EGDs) in Gaming Venues. This TSD will only concern 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 **Section 5**.*

1.4 Purpose of TSD

1.4.1 General Statement

The purpose of this TSD is as follows:

- To eliminate subjective criteria in analyzing and certifying MCS and Validation System operation.
- To test those criteria which impact the credibility and integrity of MCS and Validation System operation from both the Revenue Collection and game play point of view.
- To create a TSD that will ensure that MCSs and Validation Systems in gaming venues are fair, secure, auditable, and able to operated correctly.
- To recognize that non-gaming testing (such as Electrical Testing) should not be incorporated into this TSD but left to appropriate test laboratories that specialize in that

- type of testing.
- e) To recognize that except where specifically identified in this TSD, testing is not directed at health or safety matters. These matters are the responsibility of the manufacturer of the equipment.
 - f) To construct a TSD that can be easily changed or modified to allow for new technology.
 - g) To construct a TSD that does not specify any particular method or technology (e.g.: choice of algorithm for random number generation). The intent is instead to allow a wide range of methods and technologies to be used to comply with this TSD, while at the same time, to encourage new methods and technologies to be developed.

1.4.2 No Limitation of Technology

One should be cautioned that this TSD should not be read in such a way that limits the use of future technology. The TSD should not be interpreted that if the technology is not mentioned, then it is not allowed. As new technology is developed, GPEB, in consultation with BCLC, will review this TSD, make any changes deemed necessary, and incorporate new minimum standards for the new technology.

Note: Although BCLC may recommend that particular changes be made to this TSD, the ultimate authority to approve changes rests solely with GPEB.

1.4.3 Scope of TSD

This TSD will only govern MCS requirements necessary to achieve certification 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.

1.4.4 Exceptions to TSD

This TSD does not govern MCS requirements for any other form of monetary transaction. This TSD 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 TSD 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 **Section 5**. For EGDs and MCSs that do support advanced communication protocol features which allow for credit transfer bi-directionally, BCLC and GPEB, in consultation with the Province of British Columbia, will establish unique standards in a separate TSD. This new TSD will govern both the EGD and the MCS, as these features may impact many requirements set forth in TGS1, TGS2, TGS4 and this TSD (TGS3), or mandate that new requirements must be imposed.

1.5 Other TSDs That May Apply

1.5.1 General Statement

This TSD covers the minimal requirements of an MCS or Validation System, and all associated components. The following other TSDs and documents may apply:

- a) TGS1 – Technical Gaming Standards for Electronic Gaming Devices (EGDs) in Gaming Venues;
- b) TGS2 – Technical Gaming Standards for Progressive Gaming Devices in Gaming

- Venues;
- c) TGS4 – Technical Gaming Standards for Electronic Bingo Systems in Gaming Venues;
 - d) The Criminal Code of Canada; and
 - e) The Gaming Control Act of British Columbia.

2 Submission Requirements

2.1 Introduction

2.1.1 General Statement

This section shall govern the types of information that are, or may be required to be submitted by the submitting party in order to have equipment tested to this TSD. Where the information has not been submitted or is not otherwise in the possession of BCLC (together with GPEB) and/or the ATF, the submitting party shall be asked to supply additional information. Failure to supply the information can result in denial in whole or in part of the submission and/or lead to testing delays.

Note: The testing of the submission may take place in the BCLC testing facilities, or at the ATF's facilities, or both, at the discretion of BCLC.

2.1.2 Previous Submission

Where BCLC and/or the ATF has been previously supplied with the information on a previous submission, duplicate documentation is not required, provided that the previous information is referred to by the submitting party, and those documents are easily located at BCLC's facilities, GPEB's facilities and/or the ATF's facilities. Every effort shall be made to reduce the redundancy of submission information.

2.2 Prototype (Full Submission) Submissions

2.2.1 General Statement

A Prototype (full submission) submission is a first time submission of a particular piece of hardware or software that has not previously been reviewed by BCLC (together with GPEB) and/or the ATF. For Modifications of previous submissions, including required changes to previously submitted Prototype (full submission) certification, whether certified or pending certification, see **Section 2.7 Submissions of Modifications (Partial Submissions) to a Previously Certified Item**.

Note: Due to abnormal component complexity and/or excessive cost it may be necessary for on-site testing of a system at the manufacturer's facility. Regular upgrades normally preclude testing at the manufacturers' facility except in the case of prototype submissions.

2.2.2 Submission Letter Requirements

Each submission shall include a request letter, on company letterhead, dated within one (1) week of the date the submission is received by BCLC (together with GPEB) and/or the ATF. The letter should include the following:

- a) A formal request for certification specifying British Columbia as the jurisdiction for which the device will be approved; and
- b) The items requested for certification. In the case of software, the submitting party shall include Identification (ID) numbers and revision levels, if applicable. In the case of proprietary hardware, the submitting party shall indicate the manufacturer, model, and part and revision numbers of the associated components of hardware; and
- c) A contact person who will serve as the main point of contact for engineering questions raised during evaluation of the submission. This may be either the person who signed the letter or another specified contact.
- d) If a wireless network solution is desired, then the design and scope of the wireless solution needs to be reviewed for security considerations. Upon installation at the gaming

venue location, an independent network security auditing company (or qualified ATF) may be asked to review the installation and security procedures.

2.3 System Hardware Submission Requirements – Prototype (Full Submission) Certification

2.3.1 Presentation of Equipment to BCLC, GPEB and/or the ATF; Identical Equipment

Each item of gaming equipment supplied by a manufacturer to the field shall be functionally identical to the specimen tested and certified. For example, an interface element supplied as a certified device shall not have different internal wiring, components, firmware, circuit boards, circuit board track cuts or circuit board patch wires from the certified specimen, unless that change is also certified, see also **Section 2.7 Submissions of Modifications (Partial Submissions) to a Previously Certified Item**.

2.3.2 Inventory of Equipment to BCLC, GPEB and/or the ATF

Each submission of hardware shall contain the following:

- a) Server, Database, Front End Controller, Data Collector and Ancillary Stations to include but not limited to: Jackpot/Fill functionality; Surveillance/Security monitor functionality; EGD Management functionality; and Accounting/Reporting Functionality;
- b) Monitors, keyboards, mouse, printers, etc., to support the items listed above;
- c) Minimum of seven interface element devices with corresponding power connectors (if separate from harness), keypads, and displays;
- d) Minimum of one wiring harness for each EGD type desired for operational approval with system where specific harnessing is required;
- e) Minimum of two of each type magnetic cards (or equivalent if an alternative media is used) used in the system, if applicable;
- f) Network cabling, hubs, switches and any wireless components that may be installed at a gaming venue property; and
- g) Uninterruptible Power Supply (UPS) for critical components.

Note: In an effort to reduce system submission size, monitor and data switches may be used. Additionally, separate software may be housed in the same unit, as long as the functionality is not impaired and the software is identical to the field version.

2.3.3 Accompanying Documentation

All accompanying technical documents, manuals, and schematics shall be submitted. In addition, the following items shall be provided:

- a) If applicable, all UL, CSA, etc. or equivalent certification, see also **Section 6.2 Hardware and Player Safety**. This certification information may be supplied at a later date;
- b) Any other proprietary equipment that may be used in the field in conjunction with the Submission, if necessary to test the requirements set forth;
- c) Accompanying software, see also **Section 2.4 System Software Submission Requirements – Prototype (Full Submission) Certification**; and
- d) If the submitting party has specialized equipment and/or software which is needed to test the submitted system, such as load/game simulators or test data files, then the specialized equipment and/or software and all appropriate operation and user manuals for the equipment and/or software shall be included with the submission.

Note: Commercially available products are not required for submission unless omission will impact testing and proper operation of the system.

2.4 System Software Submission Requirements – Prototype (Full Submission) Certification

2.4.1 General Statement

Each submission of software shall contain the following:

- a) Two sets of all Erasable Programmable Read Only Memory (EPROM) devices, Compact Disk Read Only Memory (CD-ROM) devices, or other storage media which contain identical contents. This includes all program executables, system component firmware, bin files, etc. Where BCLC and/or the ATF have already tested a software component, resubmission may not be necessary (pending approval by GPEB);
- b) Source Code, a Link Map and Symbol Table for all primary software executables. In addition, if requested, explanation of all non-volatile Random Access Memory (RAM) on any system device with the non-volatile RAM locations described (Note: The source code may be reviewed, compiled and studied, at the BCLC testing facilities, or at the ATF's facilities, or both, at the discretion of BCLC);
- c) All user manuals in both hard and soft copy format to include a general overview of the system from a component level, software and hardware setup and integration, and system block diagrams and flow charts for the communication program, if required;
- d) If not included in the user manuals, a connectivity manual for all unique EGDs capable of being interfaced with system to include device model numbers and compatibility list, if applicable; wiring diagrams depicting connection points to devices, power, etc.; and identification by part number or some other scheme, any unique wiring harnesses, ancillary boards required for communication of a particular device;
- e) If not included in the user manuals, provide example reports for each standard report capable of being generated on the system with a formula summary detailing all reporting calculations including data types involved, mathematical operations performed, and field limit;
- f) If not included in the user manuals, a list of all supported communication protocols specifying version, if applicable;
- g) If utilizing a software verification algorithm provide a description of the algorithm, theoretical basis of the algorithm, results of any analyses or tests to demonstrate that the algorithm is suitable or the intended application, rules for selection of algorithm coefficients or "seeds", and means of setting the algorithm coefficients or "seeds," and
- h) If completed by the manufacturer provide a system test plan and results to detail EGDs and software versions tested with.

2.5 Software Programming Requirements and Compilation

2.5.1 General Statement

The following items shall be contained within all submitted source code or related modules:

- a) Module Name;
- b) Brief description of module function; and
- c) Edit History, including who modified it, when and why.

2.5.2 Source Code Commented

All source code submitted shall be commented in an informative and useful manner.

2.5.3 Source Code Completeness

All source code submitted shall be correct, complete and able to be compiled.

2.6 Program Identification

2.6.1 Software Requirements

On the primary system software components submitted and subsequently placed in the field, each program shall be uniquely identified and either display version information at all times or utilizing a user accessible function.

2.6.2 Firmware Requirements

On the system firmware submitted and subsequently placed in the field, each program shall be uniquely identified, displaying:

- a) Program ID;
- b) Manufacturer;
- c) Version number;
- d) Type and size of medium (requirement can be met by manufacturer stamp); and
- e) Location of installation in interface element or other system device, if potentially confusing.

Note: For EPROM based firmware, the identification label shall be placed over the UV window to avoid erasing or alteration of the program.

2.7 Submissions of Modifications (Partial Submissions) to a Previously Certified Item

2.7.1 General Statement

For any update submission (e.g., a revision to an existing hardware or software that is currently under review, certified or has been reviewed and not certified), the following information shall be required to process the submission in addition to the requirements set forth in **Section 2.2.2 Submission Letter Requirements**. All modifications will require review and re-testing to verify compliance with the applicable requirements set forth in this TSD, as per **Section 1.1.1 General Statements I**.

2.7.2 Modification of Hardware

Each hardware submission shall:

- a) Identify the individual items being submitted (including part number);
- b) Supply a complete set of schematics, diagrams, data sheets, etc. describing the modification along with the reason for the change(s); and
- c) Provide the updated or new hardware, a description and the method of connection to the original system or hardware components.

2.7.3 Modification of System Software Functions or to Correct Software Error

The submitter should use the same requirements as **Section 2.4 System Software Submission Requirements – Prototype (Full Submission) Certification** above, except where the documentation has not changed. In this case, a resubmission of identical documents is not required. However, the submission must include a description of the software change(s) and modules affected, and new source code for the entire program, if applicable

2.7.4 Software Submission - Modification to Existing or Create New System Functionality

For a system specific submission (e.g., new workstation software), the following information may be required to process the submission:

- a) If new, a complete description of the function, including amendment manual and user documents, and new source code if applicable; and
- b) If modifying, the submission must include a description of the software change(s), modules affected and new source code, if applicable.

2.8 System Security Submission Requirements

2.8.1 General Statement

Where a system requires the use of defined user roles with associated passwords or pin numbers, a default list of all users and passwords or pin numbers must be submitted including a method to access the database.

2.9 Joint Venture Submissions

2.9.1 General Statement

A system is considered a joint venture when two or more companies are involved in the manufacturing of one system. Due to the increasing amount of joint venture submissions (more than one supplier involved in a product submission) and to alleviate any confusion to the suppliers, the following procedures must be followed for such submissions (pending approval by GPEB).

- a) One company will prepare and submit the entire submission, even if they are using parts from other suppliers, and must identify all part numbers of all components. This will be the primary contact for the submission.
- b) The company submitting an approval request should do so on their letterhead. BCLC and/or the ATF will delegate an internal file number in this company's name and may bill this company for all costs incurred throughout the evaluation and approval process.
- c) The primary contact will be called when questions arise. However, BCLC will work with all parties involved, completing the review.
- d) All suppliers who are part of the submission "group" may need to be registered in British Columbia.
- e) Upon completion, it is the primary contact company that will receive the approval letter, provided the submission meets the requirements set out in this TSD as well as those requirements set out in any other applicable TSD. The primary contact company may then release copies of the approval letter to the associated manufacturer(s).

3 System Component Requirements

3.1 Interface element Requirements

3.1.1 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.

3.1.2 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 should be capable of being reviewed on demand, at the interface element level via an authorized access method, see also **Section 4.3 Meters**.

3.1.3 Battery Backup Requirements

The interface element must retain the required information after a power loss for a period determined by BCLC and BPEB. If this data is stored in volatile RAM, a battery backup must be installed within the interface element, see also **Section 4.3 Meters**.

3.1.4 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 4.2 Significant Events** and **Section 4.3 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.

3.1.5 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 should not allow for duplicate EGD file entry of this identification number.

3.1.6 Configuration Access Requirements

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

3.2 Front End Controller and Data Collector Requirements

3.2.1 General Statement

A 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 4.1** of this TSD. If the FEP maintains buffered/logging information, then a means shall exist which prevents the loss of critical information contained herein.

3.3 Server and Database Requirements

3.3.1 General Statement

A 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.

3.3.2 System Clock

A 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 shall 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.

3.3.3 Synchronization Feature

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

3.3.4 Database Access

The MCS shall have no built-in facility whereby a gaming venue user can bypass system auditing to modify the database directly. Gaming Venue Service Providers will maintain secure access control.

3.4 Workstation Requirements

3.4.1 Jackpot/Fill Functionality

A MCS System 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.

3.4.2 Large Cash Transactions Reporting (LCTR) Threshold

It should be noted that submissions under this TSD must take into account that 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.

3.4.3 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 (as approved by GPEB).

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

3.4.4 Surveillance/Security Functionality

A MCS shall 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 shall 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.

3.4.5 EGD Management Functionality

A 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 EGD.

3.4.6 Accounting Functionality

A MCS must have an application or facility that allows controlled access to all accounting (financial) information and shall be able to create all mandatory reports in **Section 4.4 Reporting Requirements**, as well as all Internal Control required reports, if specified.

3.4.7 Exclusions

Generally, any system (component) not specified in this TSD that impacts revenue reporting must be submitted to BCLC and/or the ATF for testing, and must be approved by GPEB. For example, Standalone Player Tracking Systems are not required for submission unless their function includes embedded feature(s) that affect revenue. However, they may be tested for operation and version control if an integrated feature of a MCS submission.

4 System Requirements

4.1 Communication Protocol

4.1.1 General Statement

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

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

Note: This TSD do not preclude the use of RF 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.

4.2 Significant Events

4.2.1 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 which the event occurred;
- b) Identity of the EGD that generated the event;
- c) A unique number/code that defines the event; or
- d) A brief text that describes the event in English.

4.2.2 Standard Events

The following significant events must be collected from the EGD device 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 a unique message 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 a unique message 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 a 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.

4.2.3 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.

4.3 Meters

4.3.1 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.

4.3.2 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 the TGS1 – Technical Gaming Standards for Electronic Gaming Devices (EGDs) in Gaming Venues for standards for the electronic accounting meters that are to 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.

4.3.3 Clearing Meters

An interface element should not have a mechanism whereby an unauthorized user can cause the loss of stored accounting meter information, see also **Section 3.1.4 Information Buffering and Integrity Checking**.

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

4.4 Reporting Requirements

4.4.1 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.

4.4.2 Required Reports

Reports will be generated on a schedule determined by BCLC (to be approved by GPEB), 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;
 - e) Significant Event Log for each EGD; and
 - f) Other Reports, as required by individual jurisdictions.

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, please see **Section 5 Ticket Validation System Requirements**.

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

4.5 Security Requirements

4.5.1 Access Control

The 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, the MCS shall 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.

4.5.2 Data Alteration

The MCS shall 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).

4.6 Additional System Features

4.6.1 EGD Program Verification Requirements

If supported, a 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).

4.6.2 Verification Algorithm Timing

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

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

4.6.3 FLASH Download Requirements

If supported, a 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 GPEB. At this time, BCLC and/or the ATF 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 GPEB 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.

4.6.4 Remote Access Requirements

If approved by BCLC and GPEB, a MCS may utilize password controlled remote access to a 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) should 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. GPEB must grant approval for any such activities before BCLC may proceed.

4.7 Backups and Recovery

4.7.1 General Statement

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

4.7.2 Recovery Requirements

In the event of a catastrophic failure when the MCS cannot be restarted in any other way, it shall 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.

5 Ticket Validation System Requirements

5.1 Introduction

5.1.1 General Statement

A ticket validation system may be entirely integrated into a 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.

5.1.2 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 shall come from the validation system or MCS using a secure communication protocol.

5.2 Ticket Information

5.2.1 General Statement

A ticket shall contain the following printed information at a minimum:

- a) Gaming Venue 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 or 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.

5.2.2 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 is 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.

5.3 Ticket Issue and Redemption

5.3.1 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.

5.3.2 Online Ticket Redemption

Tickets may be inserted in any EGD participating in the validation system providing 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.

5.3.3 Cashier/Change Booth Operation

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

- 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.

5.3.4 Validation Receipt Information

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

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

5.3.5 Invalid Ticket Notification

The 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).

5.3.6 Offline Ticket Redemption

If the 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 as designated by the regulatory jurisdiction that will accomplish the same.

5.3.7 Wireless Hand-held Ticket Redemption

Refer to **Section 7** covering security concerns regarding wireless local area networks.

5.4 Reports

5.4.1 Reporting Requirements

The following reports shall 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.

5.5 Security

5.5.1 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 should possess a non-alterable user audit trail to prevent unauthorized access. Further, the normal operation of any device that holds ticket information shall not have any options or method that may compromise ticket information. Any device that holds ticket information in its memory shall not allow removing of the information unless it has first transferred that information to the database or other secured component(s) of the validation system.

6 System Environmental and Safety Requirements

6.1 Introduction

6.1.1 General Statement

This section shall govern the environmental and safety requirements for all system components submitted for review.

6.2 Hardware and Player Safety

6.2.1 General Statement

Electrical and mechanical parts and design principals of the EGD may not subject a player to any physical hazards. BCLC and the ATF shall NOT be responsible for Safety and EMC testing, as it is the responsibility of the manufacturer of the goods to obtain the appropriate Underwriters Laboratory (UL) / Canadian Standards Associated (CSA) certification. Such Safety and EMC testing is required under Provincial and Municipal regulations and should be researched accordingly by those parties who manufacture said devices. BCLC and the ATF shall not be responsible for, nor be liable for, these matters.

6.3 Environmental Effects on System Integrity

6.3.1 Integrity Standard

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

- a) Electro-magnetic Interference. Systems shall 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 shall 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 shall 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 will be conducted with a severity level of up to 27KV air discharge;
- c) Radio Frequency Interference (RFI). Systems shall 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 subsection 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 shall not be adversely affected by Magnetic Interference. The manufacturer should supply any documentation if the device has had Magnetic Interference testing against any recognized standard.

7 Systems using Wireless Networks

7.1 Introduction

7.1.1 General Statement

This section shall address security precautions and minimum recommendations that govern Wireless Networks. Please take note that a security audit may be performed by an independent network security auditing company (or qualified ATF).

7.2 Wireless Ethernet Communications

7.2.1 General Statement

Should a wireless Ethernet communication solution be adopted, then additional security precautions must be taken. The current wireless Ethernet technology (Wi-Fi) is vulnerable and should not be considered secure. If Wi-Fi is chosen as the communication method for the system, the following recommendations are to be considered minimum recommendations and not restrictions:

- a) The wireless access point must be physically positioned in the building, so that it is not easily accessible by unauthorized individuals.
- b) Wireless network traffic must be secured with additional encryption to compensate for the weaknesses in Wi-Fi.
- c) The keys used to encrypt the communication through the wireless network must be stored in a secure location.

7.3 Security Considerations for WLAN used with a Wired LAN

7.3.1 General Statement

The wired LAN (Local Area Network) must be isolated from the wireless (WLAN) network through the layering of additional network security methods. The following recommendations are to be considered minimum recommendations and not restrictions:

- a) The access point must not be placed directly onto the gaming venue network unless a standalone stateful packet inspection firewall is employed.