VICTORIAN CENTRAL MONITORING AND CONTROL SYSTEM REQUIREMENTS DOCUMENT

31 January 2012

Victorian Commission for Gambling and Liquor Regulation

State Government Victoria

Table of Contents

1
Glossary

This chapter sets out the glossary of standard terms and abbreviations used by the Commission and relevant to the Central Monitoring and Control System Requirements document.

Term or Abbreviation	Description
Act	Means the Gambling Regulation Act 2003 (Vic) and Regulations, as amended from time to time.
Australian/New Zealand Gaming Machine National Standards	Refer to the National Standards.
Banknote Acceptance Device	Or, banknote acceptor; a device where a player could insert banknotes to be used for credits for Game Play.
Banknote Money In	The dollar amount of a banknote inserted into a Gaming Machine.
Baseline	A snapshot of an evolving system. The baseline also defines an envelope around a system (defined by the Licensee and approved by the Commission) of which the Commission maintains verification control over. For example application files within a baseline would need approval prior to being modified, and there must be a method in place to verify baseline files have not changed since the last approval).
Cashbox	A coin storage device that is filled when the Hopper is filled to a certain capacity. A Cashbox does not have facilities for dispensing coins.
Cash Clearance	The act of legally removing coins and notes from Gaming Equipment.

Term or Abbreviation	Description
Cashier Station	A device for which the purpose is to receive or disburse money or credit, that is associated in any way with a Gaming Machine, Significant Game Play Transactions or gaming activities. The security requirement for a Cashier Station will depend upon the functionality of the Cashier Station.
CD-ROM	Compact Disc Read-Only Memory.
Central Site	The location of the Host CMCS; a storage device that contains data accessible to, but not writable by, a computer.
CMCS	The Central Monitoring and Control System, made up of Host CMCS, Venue CMCS and network components, of the Licensee's gaming monitoring network as referred to in Section 3.1.6 of the VCR, this document.
CMCS Equipment	The equipment referred to in Section 3.1.6 of the VCR, this document.
Coins To Hoppers	The monetary amount of coins inserted into a Gaming Machine that goes into the Hopper.
Coins To Cashbox	The monetary amount of coins inserted into a Gaming Machine that goes into the Cashbox.
Commencement Date	Means the Commencement Date defined in the Licence and Related Agreements.
Commission	The Victorian Commission for Gambling and Liquor Regulation established under the Act or any successor body.
Commission Standards	The relevant Commission gaming standards consisting of the: • Australian/New Zealand Gaming Machine National Standard; • Victorian Appendix to the Australian/New Zealand Gaming Machine National Standard; and • Victorian Central Monitoring and Control System Requirements (this document).

Term or Abbreviation	Description
Communications Controller	A system component connected to the CMCS that links and manages communication between Venue-based Gaming Equipment and network components, the Venue CMCS and the Host CMCS.
Configuration Management	The process of creating and maintaining a record of all the components of the infrastructure, including hardware, software and related documentation, and managing changes to the attributes of the components.
Critical Data	Memory locations storing information including, but not limited to: • Security events of Type R which have not been forwarded to the Host CMCS; • Jackpot parameters, meters and amounts; • Mandatory metering information; • Current Game information; • Cash tickets, where maintained by the Monitoring Equipment; • Any changeable configuration information; and • Current credit amount; and • Any data associated with the Cryptographic Data Security requirements identified at 9.2.4 of this document.
Critical Memory	Non Volatile Memory that does not lose its contents when the equipment is powered off.
Cryptographic Data Security	Refers to the protection of critical communication data from eavesdropping and/or illicit alteration.
Custom Built	An item made specifically by or for the Licensee to the Licensee's specifications.
Cyclic Redundancy Check (CRC)	A non-secure hash function designed to detect accidental changes to raw computer data.

Term or Abbreviation	Description
Data	Means all data and expressions of data contained in, or processed or generated by, the legacy system or the Monitoring System including without limitation: • All data and expressions of data comprising reports generated by the legacy system or the Monitoring System; and • All data and expressions of data about or relating to or generated by agents and contractors stored within the legacy system or the Monitoring System.
De-activation	De-activation refers to the process of disabling a part of the CMCS.
Diversion Pool	Where a portion of jackpot contributions is redirected to another pool so that when the current jackpot is won, this pool is added to the restart level of the next jackpot.
Down_Time_ Permitted	The period of time a Site Controller is permitted to allow gaming to continue when the link to the Host CMCS is not operational. The default is one day.
EGM	Electronic Gaming Machine – has the same meaning as Gaming Machine.
EGM Interface Card	An Interface Card that resides inside a Gaming Machine.
EGM Protocol	The means of communication between the Venue Monitoring Equipment and a Gaming Machine in the Venue. The protocol specification will define, at least, hardware interface, line discipline(s) and message formats.
Electrostatic Discharge (ESD)	The sudden and momentary electric current that flows between two objects at different electrical potential that may cause damage to electronic equipment.
EMI	Electro Magnetic Interference - the physical characteristic of an electronic device to emit electronic noise either into free air, onto the mains power lines, or communication cables.

Term or Abbreviation	Description
EPROM	Erasable Programmable Read Only Memory. A storage device that may be filled with data or information, which once written is not modifiable (except by the application of Ultra Violet (UV) light), and where the contents are retained even if there is no power applied to the device.
External Jackpot Display Interface	A device which collects information from a Jackpot Controller and processes it into a format which is suitable for the Jackpot Display.
Firewall	Part of a computer system or network that is designed to block unauthorised access while permitting authorised communications.
Fixed Prize Jackpot	A jackpot where the winner is paid a fixed amount, cash or merchandise, which was advertised in advance.
Flash Memory	A non-volatile computer storage that can be electrically erased and reprogrammed.
Game	A Game is a sequence of actions and outputs initiated through player interaction with the device on which the Game is played. Major constituents of a Game are: rules, artwork (virtual or static and inclusive of symbols and pay-table), winning combinations and symbol distribution. Each Game has its own unique Game ID. Each different pay-table is regarded as a different variation of the Game, and has its own unique Variation ID.
Game Determined Jackpot	A jackpot that is triggered as a result of the outcome of a Game.
Game Play	Refer to Play.
Gaming Day	The hours a Gaming Venue is licensed to operate.
Gaming Device	Any piece of equipment that provides the functionality of Gaming Equipment.
Gaming Equipment	Has the same meaning as defined in the Act.
Gaming Machine	Has the same meaning as defined in the Act.

Term or Abbreviation	Description
Gaming Monitoring Activities	Means the establishment, operation and maintenance of the Monitoring System, the provision of Monitoring Services and the sale, supply and possession of Monitoring Equipment in accordance with section 3.4.4(1)(a), (b) and (c) of the Act and the Scope of Services set out in the Licence and Related Agreements.
Gaming Venue	Has the same meaning as Venue.
Hard Meter	An electromechanical meter or an electronic increment meter.
Hardware	All physical components (electrical and mechanical) making up the Monitoring Equipment.
Help Desk	A service by the Licensee that provides information and assistance to CMCS network users.
Hopper	A coin storage device that has facilities for dispensing coins.
Host CMCS	The centrally located component(s) of the CMCS that controls the CMCS and provides information and services to other components of the CMCS.
ICT	Information Communications Technology – a generic name used to describe all technologies used by computers to communicate.
Implementation Completion Date	Means the Implementation Completion Date defined in the Licence and Related Agreements.
Inspector(s)	A person who is appointed under Section 10.5 of the Act to represent the Commission in undertaking inspections of the CMCS.
Interface Card	A computer device which is located inside gaming equipment, such as an Gaming Machine, which performs various functions such as protocol conversion.
I/O Channel	The physical interface that controls the transfer of data between the computer and peripheral devices.
Jackpot	Has the same meaning as defined in the Act.
Jackpot Arrangement	An arrangement that has been approved by the Commission for operating a type of Jackpot.

Term or Abbreviation	Description
Jackpot Controllers	A system component to allow a Gaming Machine to participate in a Jackpot.
Jackpot Display	A Jackpot display provides information to players, in relation to a jackpot, such as current jackpot amounts, jackpot winners etc.
Jackpot Meter Information	Data collected by the Jackpot Controllers or an EGM.
Jackpot Pool	An accumulated reservoir of jackpot monetary contributions.
Jackpot Pool Accrual	Means the sum of the Jackpot Pool minus the amount of the Jackpot payout.
Jackpot Reset Period	The time taken to: • Register that a jackpot has been won, • Lock up the winning device, and • Reset the progressive meter.
Jackpot System	A system to allow the operation of a Jackpot, typically made up of: • Jackpot Controller; • Jackpot Display Interface; • Jackpot Display; and • Network components.
LAN	Local Area Network, a computer network covering a small physical area.
Legacy System	Means the Legacy System defined in the Licence and Related Agreements.
Licence	Means the licence granted and issued under the Act by the Minister to authorise the conduct of the Gaming Monitoring Activities.
Licensee	The holder of the Licence granted and issued under the Act by the Minister to authorise the conduct of the Gaming Monitoring Activities.

Term or Abbreviation	Description
Logic Area	The logic area is a locked cabinet area (with its own locked door) that houses electronic components that have the potential to significantly influence the operation of Gaming Equipment and Monitoring Equipment.
Master Controller	A device which is used to control Slave Controllers.
Memory	An area of a computing device used to store data and/or instructions.
Meter	A "meter" may be any of the following: • A Hard Meter. The meter can only be incremented. Meter incrementing can only be performed by the Gaming Equipment's computer. The meter is read by human inspection of the meter display. • A storage area within some form of computer Memory (e.g. disk or RAM) into which the computer's software is programmed to store and update the current count of the metered quantity.
Meter Width	The number of digits or bits of storage of the meter, so as to cater for a particular range of meter counts.
Minister	The Victorian Minister for Gaming.
Monitoring Equipment	Has the same meaning as defined in the Act.
Monitoring System	Means the electronic monitoring system referred to in section 3.4.4 of the Act and includes, without limitation, all adaptations, modifications, enhancements to that system made at any time before or during the Term.
Mystery Jackpot	A jackpot where the determination of the jackpot win is not related to the Game outcome but instead by some non-Game determined event, generally by a random event.
National Standards	The core requirements, common to all jurisdictions, for the design of Gaming Machines and games for operation throughout Australia and New Zealand and to guide testers in their testing for compliance with the standard.

Term or Abbreviation	Description
Network Policy Document	A document describing the network topology of the CMCS and is the responsibility of the Licensee to prepare as part of its submission to the Commission when obtaining approval for the CMCS.
NTU	Network Termination Unit (interface device to a wide area data network).
Off The Shelf	Software or hardware, generally technology or computer products, that are ready-made and available for sale, lease, or license to the general public – also referred to as Commercial, Off The Shelf (COTS).
On-line Significant Event	The types of Significant Event described in the Victorian Appendix to the National Standards, and Section 10 of the VCR, this document. Refer to the Glossary for the definition of Significant Event.
Peripheral Equipment	An external device, such as a printer, a disk drive, or a keyboard, connected to a Host CMCS or Venue CMCS component.
PID	Player Information Display.
PIN	Personal Identification Number.
Play	A Play is a sequence of actions and outputs initiated through a bet and terminated when the final transfer to the player's credit meter takes place (in case of a win) or when all credits wagered or won that have not been transferred to the credit meter are lost. Games that trigger a free Game feature and any subsequent free Games are to be considered as one Play.
Pre-commitment	A mechanism to allow players to stay in control of their gambling and make informed decisions about their play.
Progressive Jackpot	A jackpot arrangement where the prize is calculated by accumulating contributions.
PROM	Programmable Read Only Memory - a form of digital Memory where the setting of each bit is locked by a fuse or anti-fuse.
PSD	Program Storage Device.

Term or Abbreviation	Description
RAM	Random Access Memory - the storage facility used by the CPU to store data and instructions. This form of storage is volatile: if the machine in which it is installed loses power, the contents of RAM are lost.
Re-activation	The activation of a part of the CMCS that was previously de-activated.
Related Agreements	Means the Related Agreement, the Ancillary Documentation, the Tripartite Deeds, the Venue Monitoring Services Agreements and any additional agreements dealing with matters relating to the Licence that the Minister requires to be entered into with the Minister or a person nominated by the Minister, the Monitoring Licensee and, if applicable, others from time to time.
Responsible Gambling Ministerial Advisory Council	The pre-eminent source of stakeholder advice to the Minister on responsible gambling.
Re-Used Legacy System Components	Means the Re-Used Legacy System Components defined in the Licence and Related Agreements.
Revision Level	A term used in Configuration Management and Version Control. A Revision Level defines a baseline configuration of a system. Changes may be identified by a number or letter code, termed the “revision number”, “Revision Level”, or simply “revision”.
RFI	Radio Frequency Interference - the ability to influence an electronic device by means of using radio waves.
RNG	Random Number Generator - a method of producing a sequence of random numbers.
Roll of Manufacturers, Suppliers and Testers	Has the same meaning as defined in the Act.
ROM	Read-only Memory.

Term or Abbreviation	Description
RTP	Return to Player - The ratio of total wins (including progressives and other features) to the total turnover in a Game cycle (note: gamble bets do not affect turnover and total wins is only affected by the final gamble outcome).
Self Audit Check	An audit check similar to Gaming Machines for their appropriate meters or meters received from Gaming Machines (refer section 3.3 of the National Standards).
Significant Event	Has the same meaning as defined in the Act.
Significant Game Play Transaction	Has the same meaning as defined in the Act.
Site Controller	A device used to collect information from each Gaming Machine.
Slave Controller	A device which controls an aspect of gaming which is otherwise controlled by a Master Controller. For example, a CMCS may perform overall control of a jackpot scheme, but a Slave Controller would only perform localised control.
Stand-alone Jackpot	A jackpot where participation, maintenance and control of the jackpot, including selection of the jackpot win criteria is performed by a single Gaming Machine. The Gaming Machine may have one or more jackpots associated with it, including some linked jackpots.
System Baseline Document	Document detailing the system software and hardware components and network and communication that enable the system to operate in a secure environment and meet the legislative requirements.
Tester	Means a tester listed on the Roll of Manufacturers. Suppliers and Testers as described in the Chapter 3 of the Gambling Regulation Act 2003,
TFA	Terminal Financial Adjustment - An operations task carried out when (for example) a Gaming Machine undergoes an unrecoverable Memory corruption, and if the Gaming Machine has not been polled recently, there will most likely be outstanding soft meter data lost. Thus alternate metering information such as Hard Meter reads are used to adjust the information back into the Host CMCS.

Term or Abbreviation	Description
Touch Screen	A video monitor with a special surface screen that can interact with the user of a gaming device by touching the screen's surface.
UPS	Uninterruptible Power Supply (a no-break mains power supply including battery backup equipment).
VCGLR	The Victorian Commission for Gambling and Liquor Regulation.
VCR	Victorian Central Monitoring and Control System Requirements.
Venue CMCS	Components of the CMCS located within a Venue.
Venue Operator	The holder of a Venue Operator's Licence, a Licence issued under Division 2 of Part 4 of Chapter 3 of the Act, as defined in the Act.
Venue	Any approved Gaming Venue as defined in the Act.
Venue Signage	Non-gaming based displays within a Venue, e.g. promotional poster, responsible gambling messages, etc.
Version Control	The management of changes to documents, programs, and other information stored as computer files. Also known as revision control, source control or source code management. May be identified by a number or letter code, termed the "revision number", "Revision Level", or simply "revision".
Victoria	The State of Victoria.
Victorian Appendix to the National Standards	Details the additional requirements to the National Standards that are specific to Victoria.
Victorian Government	The Government of Victoria. Legislative power rests with the Parliament of Victoria, which consists of the Crown, represented by the Governor of Victoria, and the two Houses, the Victorian Legislative Council and the Victorian Legislative Assembly.

Term or Abbreviation	Description
Victorian Technical Standards	Means the current versions of the: • Victorian Central Monitoring and Control System Requirements document issued by the Commission, as amended by the Commission from time to time (this document); • Australia/New Zealand Gaming Machine National Standard (National Standard); and • Victorian Appendix to the Australia/New Zealand Gaming Machine National Standard (Victorian Appendix).
WAN	Wide Area Network, a computer network that covers a broad area.
Wide-area Jackpot	A Jackpot which links Gaming Machines in multiple Venues in Victoria.

2
Foreword

This chapter introduces the background to the Victorian Central Monitoring and Control System Requirements document.

2.1 Victorian Central Monitoring and Control System

2.1.1 On 10 April 2008, the Minister for Gaming announced the proposed new industry structure for Gaming Machines post 2012.

2.1.2 Under the proposed arrangements, a single Licence will be offered to an independent monitor who will provide and operate a fit for purpose monitoring system to, among other things, monitor Gaming Machine transactions in Venues.

2.1.3 The objective of the Victorian Central Monitoring and Control System (CMCS) is to ensure the integrity of Gaming Machine transactions in Gaming Venues and to provide Data and information on Gaming Machines for regulatory, taxation and research purposes.

3 Introduction

This chapter introduces the context and the purpose of the Victorian Central Monitoring and Control System Requirements document.

3.1 General Information

3.1.1 This document must be read in conjunction with the Licence and Related Agreements.

3.1.2 This Victorian CMCS Requirements document (VCR) contains the system related requirements for the CMCS which includes the Monitoring System, Jackpot Systems, Legacy System, Re-Used Legacy System Components and communication protocol requirements. It replaces the former standard, the Victorian Systems Document (VSD), for standards relating to the operation of the CMCS in the new structure commencing in 2012.

3.1.3 This document will be used by the Licensee and a Tester to evaluate the system for compliance with the CMCS requirements, or to evaluate changes to a previously approved system for approval.

3.1.4 This document will be used by the Commission to evaluate compliance by a Licensee with the Licence and Related Agreements, and to evaluate changes to a previously approved CMCS, in accordance with the Gambling Regulation Act 2003 (the Act).

3.1.5 All references in this document pertaining to the Licensee refer to the entity licensed to conduct the monitoring activity identified by its Licence.

3.1.6 The CMCS consists of any instrument, contrivance or computer hardware or software or any other equipment that the Licensee proposes to use, or will cause or permit to be used for the conduct of the activities permitted by the Act and, the Licence and Related Agreements.

3.1.7 The VCR also applies to any gaming systems that may connect to the Gaming Machines, if they are part of the CMCS that provide gaming facilities.

3.1.8 Copying or reproducing this document (or any part of this document) for commercial gain, without prior permission is prohibited.

The Act

3.1.9 The requirements specified in this document are supplementary to and do not take the place of any of the requirements of the Gambling Regulation Act 2003 (referred to as ‘the Act’) or any regulations made under the Act. To the extent of any conflict, the requirements of this document take precedence over the conditions of the Licence and any Related Agreements conditions.

3.1.10 In approving the CMCS or changes to an approved system, the Commission may take into account the certificate of a Tester under the section of the legislation applicable to the Gaming Monitoring Activities.

Objectives

3.1.11 The Commission sets high systems integrity standards for Gaming Equipment and Monitoring Equipment operating in Victoria for the purpose of ensuring that:

i) The system operates in accordance with the Licence and Related Agreements;

ii) The system operates in a manner that is auditable, reliable and secure; and

iii) All parties receive their correct entitlement.

3.1.12 Matters arising from the testing of Monitoring Equipment that has not been addressed in this document will be resolved at the sole discretion of the Commission as part of the approval process. In considering any new technology or omissions the Commission may take into account advice on such matters from either a Licensee, or a Tester, or both.

Document Scope

3.1.13 The requirements in this document apply to equipment and systems to be operated by the Licensee according to the Licence and Related Agreements at central locations and Venues in Victoria and at a disaster recovery site in Australia.

3.1.14 This document does not apply to casino operations.

3.2 ICT Service Management Framework

3.2.1 In order to ensure that the CMCS and associated equipment operate as approved by the Commission, the Licensee must establish and maintain policies, standards and procedures that the Licensee will use to develop, implement and operate the CMCS, including but not limited to:

i) Service desk, incorporating the Help Desk;

ii) Incident management;

iii) Problem management;

iv) Change management;

v) Release management;

vi) Configuration Management;

vii) Application management;

viii) Availability management;

ix) Capacity management;

x) Service level management;

xi) Financial management;

xii) Service continuity management;

xiii) Security management; and

xiv) ICT infrastructure management.

3.2.2 Within the ICT Service Management Framework, the Licensee must establish and maintain Quality Management Systems[1] that meet ISO 9000[2] or an equivalent standard.

3.2.3 Within the ICT Service Management Framework, the Licensee must establish and maintain Information Security Management Systems[3] that meet ISO 27000[4] or an equivalent standard.

3.3 Operational Requirements

Provision of Information

3.3.1 The Licensee must maintain and retain all records pertaining to the design, manufacture and testing of CMCS software and equipment which may be required by the Commission.

3.3.2 When evaluating the system(s) for approval, the Licensee must provide sufficient information and documentation to enable a full determination of the CMCS level of compliance with this requirements document.

[1] The organisational structure, procedures, processes and resources needed to implement Quality Management.

[2] A family of standards for Quality Management Systems.

[3] A set of policies concerned with information security management.

[4] A family of standards for information security management systems.

System Performance Standards

3.3.3 The CMCS must be capable of meeting the performance standards set out in the Licence and Related Agreements.

3.3.4 Communication systems forming part of or used in association or connection with the CMCS must be capable of meeting the performance standards set out in the Licence and Related Agreements.

3.3.5 The CMCS must operate only as approved and in accordance with the requirements of any standards, specifications or conditions determined by the Commission.

3.3.6 The CMCS must be capable, at all times, of determining whether all terminals and peripheral equipment connected to it are functioning.

Responsibilities

3.3.7 The Licensee must adhere to the responsibilities detailed in the Licence and Related Agreements.

3.4 Approved Monitoring Equipment

Approval of Monitoring Equipment

3.4.1 Only approved Monitoring Equipment may be operated in Victoria.

3.4.2 Approval must be obtained from the Commission before any equipment capable of affecting the integrity and conduct of Games, or the integrity and conduct of monitoring as determined by the Commission, becomes part of the CMCS.

3.4.3 Each component of any one Hardware Revision Level shall be identical.

3.4.4 A component of the CMCS may have multiple suppliers of major assemblies, but each component from each supplier must be approved by the Commission. Off The Shelf and Custom Built components of the CMCS are required to meet a minimum standard equivalent to the equipment submitted for approval.

Equipment Operation and Special Dispensation

3.4.5 Blank

3.4.6 From the Commencement Date and until the Implementation Completion Date, an approved Legacy System continues to be an approved system.

3.4.7 From the Implementation Completion Date, any Re-Used Legacy System Component must fully comply with all requirements specified in the Victorian Technical Standards.

4 Central Monitoring and Control

This chapter sets out the central monitoring and control requirements that must be met for the Licensee's operation in Victoria.

4.1 CMCS Environment

4.1.1 The Commission requires that the Licensee implement a computerised Central Monitoring and Control System capable of monitoring all Gaming Devices within all Victorian Venues in accordance with the Licence and Related Agreements and additional functions as determined by the Commission from time to time, and meeting the following broad functions:

4.1.2 The CMCS shall be designed in consideration of the following usability principles:

i) Visibility of system status, keeping users informed through appropriate feedback within reasonable time.

ii) Words, phrases and concepts familiar to the user, rather than system-oriented terms, in a natural and logical order.

iii) Facility to correct a mistake (undo or redo the action) without having to go through an extended dialogue.

iv) Platform conventions that ensure words, situations, or actions mean the same thing.

v) Design which prevents error-prone conditions or checks for them and presents users with a confirmation option before committing an action.

vi) Minimise the user's memory load by making objects, actions, instructions and options visible or easy to retrieve whenever appropriate.

vii) Flexibility and efficiency of use through design that caters to both inexperienced and experienced users and allows users to tailor frequent actions.

viii) Aesthetic and minimalist design that excludes information which is irrelevant or rarely needed.

ix) Help for users to recognise, to diagnose, and to recover from errors including error messages that are expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.

x) Help and documentation that is easy to search, is focused on the user's task, and lists concrete steps to be carried out.

4.1.3 The CMCS shall be designed in consideration of the Whole of Victorian Government ICT Standard for Accessibility, available from the eGovernment Resource Centre[5], maintained by the eServices Unit, Information Victoria - a unit within the Department of Innovation, Industry and Regional Development (DIIRD).

4.2 Host CMCS System Accommodation

Physical Security

4.2.1 The Host CMCS computer room(s) must be a secure area where only authorised personnel can enter. The Commission requires the adoption of an electronic locking system that provides monitoring information on the entry and exit of all personnel.

4.2.2 Procedures must be established and maintained to ensure only authorised personnel are allowed access.

4.2.3 There must be a detection system that records an audit log entry, and must provide an alert when unauthorised entry to the computer room is attempted.

Power Supply

4.2.4 All Host CMCS Monitoring Equipment and powered devices within or contributing to the computer room(s) environment must be supported by at least one UPS and at least one stand-by generator.

4.2.5 Policies, standards and procedures must be established and maintained to enable computer systems to be shut down in a controlled and auditable manner without the loss of Data, and must include provision should a UPS or stand-by generator fail.

4.2.6 If the supply of mains power to a Host CMCS component is disrupted, the component must not severely interfere with the operation of any other Monitoring Equipment, including equipment external to the Host CMCS environment.

4.2.7 The UPS, stand-by generator, emergency lighting and any systems or procedures referred to herein, or otherwise essential to the operation of the Host CMCS, must be tested at least every three months.

[5] http://www.egov.vic.gov.au

4.2.8 Testing of these procedures and facilities must be logged, and the logbook or equivalent record must be available for inspection by the Commission, and the Commission may be in attendance at any test.

Uninterruptible Power Supply

4.2.9 The computer, security and telecommunication systems within the Host CMCS must be protected against power fluctuations and temporary loss by installation of a UPS or other such device.

4.2.10 The UPS must provide sufficient supply to support the Host CMCS for up to two hours continuous power supply on full load until the generator is started, and enable the systems to be shut down in an orderly manner without the loss of Data, should the generators fail.

4.2.11 All equipment situated in the computer room must be earthed via the UPS.

Stand-by Generator

4.2.12 The Host CMCS must be protected against loss of power by the installation and maintenance of a generator or other such device. The generator must have the fuel capacity to support the computer systems, air conditioning, security system, telecommunication equipment, computer terminals, environmental monitoring system and sufficient lighting for normal operation of the Host CMCS Monitoring Equipment and facilities for a period of not less than 24 hours.

Emergency Lighting

4.2.13 The Host CMCS computer room must have an emergency lighting system that automatically lights when mains power is lost. If this operates from the UPS, there must be sufficient capacity in the UPS to cater for the lights (plus computers and air conditioning).

Environmental Monitoring System

4.2.14 All Host CMCS Monitoring Equipment within the computer room(s) environment must be supported by an environmental monitoring system that will perform automated switching to backup systems for most component failures of the environmental system.

4.2.15 The environmental monitoring system must be able to check the parameters of the environment that are required for the safe and continual working operation of the equipment and to automatically alert if these conditions are not met.

Help Desk System

4.2.16 A “Help Desk” facility must be provided to assist participating Venues and personnel with problems, disputes and maintenance calls and be available whenever gaming is scheduled in any Gaming Venue, and be available at least one hour before and at least one hour after gaming is scheduled in any Gaming Venue.

4.2.17 The Help Desk operators are to have secure on-line access to the Host CMCS to enable them to perform these activities.

4.2.18 The Help Desk system must enable direct access to multiple Help Desk operators via a call to a dedicated number. There must be sufficient capacity on this dedicated number for participating Venues and Venue Operators to establish contact with Help Desk operators during critical events without unreasonable delay.

4.2.19 All calls to the Help Desk must be logged and the log made available to the Commission upon request. The information recorded in the log must include, but is not limited to:

i) The time and date the call was made to the Help Desk;

ii) The Venue and/or Operator making the call;

iii) The issue prompting the call; and

iv) Details of the outcome of the call.

4.2.20 The Help Desk must comply with the standards specified in the Licence and Related Agreements.

4.3 CMCS System

4.3.1 Commission approval must have been obtained for the software configuration (baseline) of Monitoring Equipment.

4.3.2 Commission approval must be obtained for the baseline document, including any changes to the baseline document.

4.3.3 The assessment will evaluate the software configuration for reliability, recovery, audit ability, redundancy, and security.

System Baseline Document

4.3.4 The Licensee must prepare and maintain a System Baseline Document.

4.3.5 The Licensee will develop and define the System Baseline Document for approval by the Commission. The System Baseline Document will determine the core areas of the system (hardware and software) and will include the following components:

i) Hardware platforms;

ii) Operating systems;

iii) Host network topology (see 9.3.2);

iv) Application files and critical macros and/or scripts;

v) Interface modules with databases used by the system application;

vi) Venue Site Controllers, Interface Cards and linked jackpot equipment[6];

vii) Venue CMCS communication devices that interface with Venue-based Monitoring Equipment;

viii) The method used to verify that the system is operating in an approved configuration; and

ix) Any other special operational or procedural issues that is relevant to the Commission.

4.3.6 In order to establish a baseline document, an agreement must be reached with the Commission regarding the directories in which application files will be located on the CMCS computers. Files that cannot be verified because they change frequently are not expected to include functionality that would be in the baseline, nor be stored in system application directories.

4.3.7 The CMCS must have a method to verify the baseline system application executable files (and selected command utilities) in order to confirm that the configuration of the system is operating in an approved state.

4.3.8 There must be adequate policies, procedures and standards in place to ensure that portions of the system outside the baseline envelope (as approved by the Commission) are checked regularly to ensure that unauthorised activities are not taking place on the system.

CMCS Software Procedures

4.3.9 The Licensee must establish and maintain policies, procedures and standards in accordance with the requirement at section 3.2 of this document.

4.3.10 The operational control of the CMCS must be administered in accordance with adequate internal control policies, procedures and standards.

4.3.11 Only approved application files, within the baseline, may reside on storage devices or in the Memory of the CMCS computers.

[6] Linked jackpot equipment has the same meaning as defined in the Act.

CMCS Software Quality

4.3.12 Refer to Section 7.2.11.

4.4 Central Logging of Information

4.4.1 Game Play statistics[7], machine events and configuration Data (including configurable pay-table information where applicable) must be held for each individual Gaming Device in a (backed-up) central computer system. They may also be held in intermediate points in the CMCS or network.

4.4.2 The Data should be identified by the ID number issued under Section 3.5.8 of the Act. This should include all Data sent to remote locations (for instance, Gaming Machine level Data sent to Venues for performance monitoring and settlements).

4.4.3 All accounting and security event Data must be held and be able to be accessed or retrieved (e.g. from back-up) for:

i) Daily Venue totals for seven years;

ii) Daily Gaming Machine totals for two years; and

iii) All Significant Events for two years. See Chapter 10, CMCS Significant Events.

4.4.4 Accounting and security event Data must be held for each individual Gaming Machine as well as accumulated for each Venue.

4.4.5 Commission approval must be obtained for the units in which each statistic is to be measured but may include cents, dollars, number of coins/tokens or others.

4.4.6 Subject to the discretion of the Commission, the required accounting statistics are those described in the National Standards and in Sections 8.3.1 - 8.3.3 of this document. Where additional or separate metering is required by the CMCS protocol these meters may be derived from these relevant standards or otherwise maintained and transmitted to the Host CMCS.

4.4.7 In addition to the statistics required above, the Host CMCS must be able to report calculated player return statistics for each Game monitored by the CMCS.

Meter Wrap Handling and Meter Width

4.4.8 There must be adequate policies, procedures and standards in place which, together with the width of the meters and the expected rate of

[7] Information relating to patterns of betting and Game outcomes based on Gaming Machine type, Game type and Significant Game Play Transactions.

meter counts, are sufficient to cater for resulting meter wrap events (i.e. to detect and correctly handle meter wraps), and so preserve the true total statistics.

4.5 Significant Events

4.5.1 The Licensee must establish and maintain policies, procedures and standards for reporting Significant Events to the Commission.

4.5.2 The Significant Events are described in ‘On-Line Significant Events' in the Victorian Appendix to the National Standards, and Section 10 of this document.

Storage of Significant Events

4.5.3 The Significant Events prescribed by the Commission, regardless of the source of these events, are to be stored at the Host CMCS or intermediate points of the CMCS at the Licensee’s premises.

4.5.4 All Significant Events must be stored electronically in a manner approved by the Commission.

4.5.5 A date and time stamp (when the event occurred) must mark each record in the file and it must be possible to retrieve events in a serial fashion.

4.5.6 Significant Events may also be stored in subsidiary points of the CMCS (e.g. Gaming Machines, local controllers, remote controller, regional computers, etc.).

4.5.7 Significant Events must be detected and recorded within 10 seconds of the occurrence of the Significant Event.

4.5.8 Significant Events must be reported to the Host CMCS within 10 seconds of the recording of the Significant Event. An exception may apply under the conditions allowed in Section 7.4.2 iv)regarding a temporary break in communications between the Venue CMCS and the Host CMCS.

Recovery of Significant Events

4.5.9 In the event of the failure of the central system database it must be possible to electronically recover the Significant Events using a method that ensures no Significant Events are lost.

Creation of Significant Events

4.5.10 Where the Victorian Technical Standards or this document state that the CMCS must detect and record Significant Events, it does not imply a particular implementation. As long as the Commission can be assured that these events are detected and reported within the specified time frame, the method that is used to do this is of little concern. However, if the standards state that a Gaming Machine must detect and record an event, then the Gaming Machine or other specific Gaming Equipment must be programmed to create internally the event and pass it to the Venue CMCS as soon as it can (and possibly de-activate Game Play).

4.6 Gaming Equipment Configuration Database

4.6.1 The Licensee must maintain the following information for each Gaming Device for the Commission Gaming Equipment Reconciliation (GER) requirements:

i) Location;

ii) Device description (e.g. Serial number, manufacturer);

iii) Configuration (i.e. denomination, software version installed, Games available, progressive status); and

iv) History of upgrades, movements, and re-configurations.

4.6.2 It is the Venue Operator’s responsibility to provide the above information to the Licensee to enable the database to be maintained.

4.6.3 The requirements of this section may be achieved by the CMCS, a separate computer or manual system, or any combination thereof, but in any case the information must be provided to the Commission in the format, manner and timelines as advised by the Commission.

4.7 Retention of Unclaimed Moneys

4.7.1 Retention of unclaimed moneys must be treated in accordance with the Unclaimed Money Act 2008.

4.7.2 If there are to be “old” unclaimed monies stored on a gaming system (e.g. unclaimed cash tickets, inactive accounts), the serial number or other access method must be secured. The method used to secure the information must ensure that a program cannot be run to provide a list of unclaimed monies that might be illegally obtained.

4.7.3 The ability for the Commission to identify amounts that are unclaimed must be provided.

4.8 CMCS Security

4.8.1 The Licensee must establish and maintain policies, procedures, standards and mechanisms for adequate security over the approved system, including but not limited to virus prevention, detection, and correction to ensure continued system integrity, availability, and audit ability.

4.8.2 The operating system of the computer's application files and database must provide comprehensive access security for any access to any configuration item or function of the system including but not limited to system users, system operators, system developers and system administrators.

4.8.3 The Licensee must establish policies, procedures and standards for the use of passwords or equivalent, which must include but is not limited to:

i) Initial password change on its first use must be enforced;

ii) An appropriate minimum password length policy must be enforced;

iii) An appropriate methodology for the enforced frequency of unique password changes and restriction of password re-use;

iv) Procedures for password checking against a list of invalid names (dictionary checking); and

v) Procedures for adequate protection of emergency passwords.

4.8.4 The Licensee must establish and maintain policies, procedures and standards for internal reporting that provide for detection, prevention and correction of security configuration changes or breaches, including but not limited to:

i) Unauthorised attempts to access a system account;

ii) Unauthorised attempts to access a user account;

iii) Unauthorised attempts to access system resources;

iv) Unauthorised attempts to view or change system security definitions or rules;

v) Unauthorised attempts to add, modify or delete critical system Data;

vi) Irregular patterns of use for system or user accounts;

vii) Unauthorised changes to security configuration; or

viii) Significant authorised changes to security configuration.

4.8.5 The Licensee must establish and maintain policies, procedures and standards for security and Configuration Management of any media library administration of Data, including any arrangements relating to off-site storage.

4.8.6 All programs and important Data files must only be accessed by the entry of a password that is known only to authorised personnel, and that each authorised person must have a unique password that is encrypted in a non-reversible form.

4.8.7 The storage of passwords must comply with the Licensee's security policies, procedures and standards and must provide for an encrypted, non-reversible form.

4.8.8 A program must be available that will list all registered users on the system including their access level and a record of no less than 12 months of activity history by the registered user, and this list must be kept current and available at all times for inspection by the Commission.

4.8.9 The Licensee must ensure that access to specific functions, within the CMCS is restricted to specified users and requires the prior entry of the highest level password(s). The functions to be restricted include, but are not limited to:

i) System parameter changes;

ii) Installation of new versions of software; and

iii) Other functions as determined by the Commission.

4.8.10 The Licensee must develop and maintain policies and operating procedures to prevent hacking or unauthorised access to the CMCS and Monitoring Equipment.

4.8.11 The Licensee must ensure that an accredited external and independent Information Technology Network and Security Testing company undertakes system and network vulnerability and penetration testing on its CMCS and Monitoring Equipment every six months across a sample of Venues, as specified by the Commission and provide a written report of its findings. This report must be provided to the Commission within two weeks of its receipt and must include details of action(s) taken, and planned actions, by the Licensee with respect to all issues identified in the report.

System Audit

4.8.12 The Licensee must establish and maintain policies, procedures and standards for system audit matters, including but not limited to:

i) Adequate system security procedures and policies are in place, including security reviews conducted at least every three months;

ii) Critical issues management;

iii) Audit log monitoring, including preventative and corrective actions;

iv) Database security and control, including configurable parameters to protect the integrity of the system;

v) Software integrity;

vi) Peripheral equipment integrity;

vii) User access, including restriction of user access by menu items;

viii) Remote access, including monitoring and preventative or corrective actions for relevant security breaches;

ix) Network and communications security, including prevention, detection and correction measures for relevant security breaches;

x) System interfaces, including management of neighbouring applications, external systems, remote Venues and third party services;

xi) Production environment security, including prevention, detection and correction measures for relevant security breaches;

xii) Software change control aligned with change management processes; and

xiii) Emergency change control.

4.8.13 The Licensee must establish and maintain policies, procedures and standards for the use of data editors, utilities or related software, such as SQL, for database access or update (manual or otherwise). In any case, these must not be accessible by unauthorised persons.

Access by Commission

4.8.14 The Licensee, at the direction of the Commission or an Inspector appointed under Section 10.5 of the Gambling Regulation Act 2003, must provide online, read only access for the Commission to the Licensee's computer system.

4.8.15 The CMCS software supplied to the Commission must provide tools and mechanisms to:

i) Examine Significant Events;

ii) Examine Data; and

iii) Verify the approved system baseline.

4.8.16 The communication link between the Commission and the Licensee must be encrypted and meet the minimum standard identified in Section 4.11.1 of this document.

4.9 CMCS Recovery

Host CMCS Recovery

4.9.1 The Licensee must have policies, procedures and standards in place in accordance with Commission guidelines for Host CMCS Data and software recovery (and any relevant component of it such as a jackpot or player loyalty system). The disaster recovery site should meet the standards required for the primary site as set out in this document.

Transaction Logging

4.9.2 A complete log of transactions since the last backup is to be maintained at a disaster recovery site approved by the Commission.

4.9.3 For transaction logging it is required that:

i) The Host CMCS must record in a log file or databases (including time stamp and date stamp) all vital transactions received from Gaming Equipment, cashier stations, control stations, coin counters and other elements of the CMCS. For the purposes of this section 'vital transactions' means the transactions listed in section 4.9.15;

ii) The log file(s) and/or database must be duplicated for reliability using secure storage methodology;

iii) Commission approval must be obtained for the method of transaction logging;

iv) The method of transaction logging will be assessed prior to approval by the Commission; and

v) All adjustments or modifications to the transactions (and unclaimed monies or accounts) must be recorded with the Host CMCS operator's user ID (and time/date-stamp).

4.9.4 All transactions and events are to be serially written to the log in the order that they occur.

4.9.5 There must be no possible means of adding to, amending, "writing over" or deleting any transaction, record or Data contained in the log of existing records.

Format of Log Records

4.9.6 All log records must have a standard format that is approved by the Commission, and the following minimum information is to be included with each log record:

i) The date that the transaction/event occurred;

ii) The time that the transaction/event occurred;

iii) The identifier for the part of the CMCS for which the transaction/event occurred;

iv) Any relevant Data that is associated with the event; and

v) A unique event identifier which defines the transaction/event.

4.9.7 A list and description of all transaction/event id's must be provided to the Commission, and must be kept up to date by the Licensee as modifications are made to the system.

Disaster Recovery and Business Continuity

4.9.8 The Licensee must have disaster recovery and business continuity capability, demonstrated through adequate backup and recovery mechanisms (including total capacity to cope with peak load, fault tolerance, security and control).

4.9.9 The Licensee must establish and maintain policies, procedures and standards for business continuity and disaster recovery.

4.9.10 The Licensee must establish and maintain a business continuity plan, and a disaster recovery plan.

4.9.11 The Licensee must establish and maintain a disaster recovery test plan, including a schedule for testing, that is approved by the Commission, and conduct disaster recovery testing in accordance with the approved plan.

4.9.12 In the event of a disaster, there must be a method of ensuring that all Data and transactions and information related to Monitoring Equipment can be rebuilt up to the point of the disaster.

4.9.13 Copies of all daily database backups must be retained at a secure location other than the primary site, and the secure location must have security policies, procedures and standards equivalent to that required of the primary site.

4.9.14 There must be periodic back-ups (at least daily) of the variable database files on the Host CMCS storage devices.

System Data Recovery

4.9.15 In the event of a failure whereby the Host CMCS cannot be restarted in any other way, it must be possible to reload the database from the last backup point and fully recover at least all of the following vital transactions:

i) Significant Events;

ii) Cash tickets generated and/or cashed including current account balances;

iii) Account information including winnings, bets, cash deposits and cash withdrawal, PIN change, expiry date, site where issued;

iv) Manual database updates;

v) CMCS/Venue Operator network reconfiguration including addition of Gaming Equipment, deletion of Gaming Equipment, modification of Gaming Equipment (e.g. card to coin, different denominations, new Games), addition of Sites, deletion of Sites, line swapping;

vi) Metering statistics;

vii) Jackpot transactions including contributions, winnings and current value for each jackpot in the system;

viii) Current system encryption keys; and

ix) Jackpot parameters, modifications, reconfiguration (including participating Venues and Gaming Machines), additions, merges, deletions, transfers and display parameter changes.

4.9.16 Certain database update information of a non-critical nature may not be required to be automatically recovered. Exceptions of this nature would need first to be agreed with the Commission.

4.9.17 The method used to backup and retrieve the information must ensure that the information is secure and cannot be used or obtained illegally or in an unauthorised manner.

Central Site Failure Modes and Recovery

4.9.18 Following any failure, it must be possible to restore the state of the Host CMCS and its database(s) without losing Data as defined in Section 4.9.1 Host CMCS Recovery.

4.9.19 All backup or stand-by systems should be tested regularly to ensure the timely support of the systems.

4.9.20 Some typical tests that may be implemented by the Commission or its representatives to test compliance with this and other sections of the VCR are:

i) Failure of central processor;

ii) Failure of central computer power supply;

iii) Failure of central computer Memory;

iv) Failure of central computer disk(s);

v) Failure of central computer I/O channels;

vi) Total power failure of the Central Site for a short period, (e.g. 30 seconds);

vii) Total power failure of the Central Site for a long period, (e.g. 30 minutes); and

viii) Operator error (invalid Data entry, etc.).

4.10 Terminal Financial Adjustments (TFA)

Critical Memory Clear[8]

4.10.1 The Licensee, and also the Venue Operator, must establish and maintain policies, procedures and standards for the loss of Gaming Equipment soft meter Data in the field due to malfunctions.

Handling of Master Resets

4.10.2 The CMCS must be able to identify and properly handle the situation where master resets have occurred for Gaming Machines and Monitoring Equipment, including but not limited to:

i) Jackpot Controllers;

ii) Interface Cards; and

iii) Site Controllers.

4.10.3 The CMCS must be able to retrieve that last valid meters stored within the system before the master reset occurred.

4.10.4 There must be a method, subject to strict security control, where manual entry of lost metering / information is entered from Data manually collected e.g. from Hard Meters. The system must perform reasonableness checks against the last read meters values automatically recorded by the system.

TFA Procedures

4.10.5 Terminal Financial Adjustments (TFA), which may be required due to problems such as accidental Gaming Machine Critical Memory resets, represents both a source of error and a security risk. The following requirements apply to TFA's:

i) TFA's may only be performed by authorised personnel - i.e. access to this functionality must be password restricted;

ii) A paper trail of all input to the TFA must be maintained; and

iii) There must be a report / searching mechanism available so that all TFA's performed on the system can be identified.

[8] The process a service technician goes through to reset the Memory of a Gaming Machine, which configures the Gaming Machine in an 'as new' state.

4.11 Data Security

Encryption of Stored Data

4.11.1 The Licensee must encrypt stored Data and the encryption used must meet cryptographic standards equivalent to the standards set out for encryption in the Australian Government Information and Communications Technology Security Manual (ISM)[9].

4.11.2 As a minimum, the following information classes must be encrypted in a non-reversible form for storage and use:

i) PINs; and

ii) Passwords.

4.11.3 As a minimum, the following information classes must be encrypted (reversible) for storage for recovery purposes:

i) Encryption/decryption keys;

ii) If seed information (for signature or RNG) is not logically stored in a password-protected area of the highest access level, then this Data must also be encrypted; and

iii) Unclaimed tickets and critical fields such as serial numbers and authentication codes for tickets / vouchers that have not been claimed for a period of longer than two (2) weeks, wherever they might be stored within the CMCS.

PIN and Password Management

4.11.4 If a CMCS operator's PIN or password is used in support of the system, the PIN or password creation algorithm, its implementation and operational procedures (pertaining to PIN and password changes, database storage, security and distribution) must be evaluated by the Commission prior to approval.

4.11.5 The storage of PINs is to be in an encrypted, non-reversible form. This means that if a person (authorised or not) reads the file that stores the PIN Data, he/she must not be able to reconstruct the PIN from that Data even if the PIN creation algorithm is known.

4.12 CMCS Integrity

4.12.1 The Licensee must establish and maintain policies, procedures and standards for Configuration Management, including a Configuration Management plan that identifies the configurable items under management.

[9] http://www.dsd.gov.au/library/infosec/ism.html

4.12.2 Commission approval must be obtained for the hardware configuration of CMCS gaming systems.

4.12.3 The assessment will evaluate the hardware configuration for operational integrity as well as reliability, recoverability, audit ability, redundancy, and security.

Security of Event and Transaction Logs

4.12.4 The system must prevent the changing of the Significant Events log and/or Significant Game Play Transactions. It is mandatory that the event log and software is structured so that it is not possible for there to be unauthorised modifications. This will involve both password security control and ensuring that the only valid method of writing to the events log is output sequential (i.e. no random update methods are to be permitted).

Multiple Log Files

4.12.5 There must be at least two physical copies for each file and/or database that contains the vital information documented in Section 4.8 CMCS Security and Section 4.9 CMCS Recovery using secure storage methodology.

4.12.6 The Licensee’s security policies, procedures and standards, and the mechanisms for ensuring system security, apply equally to production Data files and databases and redundant Data files and databases.

Data and Event Collection

4.12.7 Game Play financial information and event Data must be passed to the Host CMCS by an approved electronic data communications means in a timely manner by schedule and/or on demand.

4.12.8 Guaranteeing the authenticity of this information at the Host CMCS will be one of the important aspects of the Commission's system verification and approval process.

4.12.9 Commission approval must be obtained by the Licensee for the frequency of financial verification Data collection.

4.12.10 The Commission will not approve any new monitoring systems unless the system is able to gather metering statistics at a frequency approved by the Commission so that automatic accounting updates can occur.

Documentation and Reporting

4.12.11 Details of the Commission’s reporting requirements will be provided to the Licensee by the Commission.

Required Reports

4.12.12 As a minimum the following reports will be required by the Commission:

i) Reports to verify financial gaming activity, including taxation, on all Gaming Machines (and jackpots) connected to the CMCS on a daily, weekly and monthly basis;

ii) Daily reports to identify any Gaming Machines or controllers that have undergone Critical Memory resets;

iii) Daily reports to identify Gaming Machines or controllers that have not transferred master meter information to the Host CMCS;

iv) Reports to identify each TFA performed;

v) Reports to identify what versions of PSD image files[10] are loaded on the CMCS, and if Gaming Machines or Jackpot Controllers connected to the CMCS are using a particular PSD image file;

vi) Reports to enable the Commission to verify that Games and jackpots being offered by the Venue Operators meet the requirements of the Act; and

vii) Reports of any security breach or attempted security breach of the CMCS, including but not limited to breaches or attempted breaches of a system Firewall.

4.12.13 The Commission must be satisfied that:

i) The information printed or displayed is accurate;

ii) The user interface and operation of the system is presented, both by the system and in documentation (operators manuals, etc.), in a manner which is conducive to efficient operation of the systems; and

iii) Reports that are to be supplied to the Commission must be able to be clearly printed, and available in electronic format if required.

[10] The mirror image data file of EGM or controller software that is loaded onto the CMCS for the purpose of signature checking devices in the field.

Summary Data

4.12.14 The Host CMCS must maintain and store summary Data on Games played, bets placed and prizes (including jackpots) won for each Gaming Machine.

4.12.15 The Host CMCS must maintain and store summary Data made for each Jackpot Pool of jackpot contributions, jackpot prizes won and current jackpot amounts.

4.12.16 It is mandatory that this summary Data is gathered at least daily.

4.12.17 The Host CMCS must generate a report for all Gaming Machines that did not respond to a request by the Host CMCS for the previous period's summary Data.

4.12.18 A Gaming Machine or Jackpot Controller must deactivate itself if it has not sent its summary Data to the Host CMCS for more than 54 hours in the case of a non-jackpot Gaming Machine or 30 hours in the case of a jackpot Gaming Machine or Jackpot Controller. Re-activation of a Gaming Machine or Jackpot Controller is not permitted until the Host CMCS requests and receives the summary Data.

4.12.19 This requirement of a Gaming Machine or Jackpot Controller must be met regardless of whether the Gaming Machine has had any financial transactions in that period or not.

CMCS Interface

4.12.20 Commission approval will be required before implementing the integration of all sub-systems into the CMCS. For example, this could be systems performance monitoring software, added security systems or any other application which is assisting in the efficient operation of the system.

4.12.21 The Commission will not approve any information flowing to or from the CMCS to sub-systems unless the interface is approved and is baseline.

Link to Commission Computing Facilities

4.12.22 There must be a data link from the Licensee's Host CMCS to the Commission's computer facilities.

4.12.23 The data link between the Commission and the Licensee's Host CMCS must implement Cryptographic Data Security as detailed in Section 9.1.21 of this document.

4.12.24 The data link between the Commission and the Licensee’s Host CMCS must have a minimum data transfer rate of 20 megabits per second.

4.12.25 This link is for the purpose of down loading financial, Game Play statistical Data Significant Events and jackpot Data on a daily basis (or at a frequency agreed by the Commission). Such Data must be extracted from the Host CMCS database to a special Commission database.

4.12.26 This Data must include the following:

i) Gaming Machines;

ii) Game Play and financial Data;

iii) Type 4 and other reportable Significant Events;

iv) Gaming Machine weekly movement Data;

v) Terminal Financial Adjustments;

vi) A terminal that fails to respond to the daily poll;

vii) Zero play reporting terminals;

viii) Jackpot Data;

ix) Accounts; and

x) Totals of deposits, withdrawals and adjustments.

4.12.27 The Licensee is also to provide to the Commission or an Inspector appointed under the Section 10.5 of the Gambling Regulation Act 2003, direct access to the Host CMCS from Commission premises for online interrogation of such system Data as events, meters, jackpots and financial Data. Such access must be read-only i.e. the Commission’s representative should have no capability to alter any Data on the system.

Inspection

Facilities for Inspectors

4.12.28 Facilities for Inspectors are to include as a minimum the following:

i) Ability to determine operational hardware and software Revision Levels;

ii) Ability to view down-loadable software or payout tables, where applicable;

iii) Ability to perform signature checks;

iv) Ability to verify that Gaming Machines and other equipment are on-line;

v) Facilities to support an inspector working together with an inspector in the field;

vi) Other facilities to assist the conduct of inspectors' tasks as necessary for a particular gaming system;

vii) Provision for technical assistance to perform all the above;

viii) Ability to review financial meters and (or) Data;

ix) Facilities (v) and (vi) to include provision and maintenance of hardware and electronic links at and to the Commission's premises; and

x) Provision of technical assistance on request from the Commission to assist Commission Inspector's in the conduct of technical compliance.

4.13 Link to External Gaming Systems

Requirement

4.13.1 The CMCS must be capable of facilitating a real time link from the Venue CMCS to one or more gaming service providers to communicate meter and event information and enable specific gaming activities.

Link Protocol

4.13.2 The Licensee must establish and maintain policies, procedures and standards for links to external gaming systems.

4.13.3 An interface document which specifies the interface including hardware, protocol and message formats must be prepared and submitted by the Licensee as part of or together with the System Baseline Document (Section 4.3.4), to the Commission for approval.

4.13.4 The interface specification document, once approved, must be made available to approved suppliers of gaming systems.

4.13.5 All communications within the link(s) must meet the principles of the network and communications requirements established in Section 9 including but not limited to the Cryptographic Data Security and secure communication principles established in Section 9.2 and the network principles established in Section 9.3.

4.13.6 The data link between the Licensee's Venue CMCS and an external gaming system must have a minimum data transfer rate of 20 megabits per second unless otherwise agreed by the Commission.

Link Approval

4.13.7 Approval by the Commission for a link to an external gaming system will be based on consideration of, on a case by case basis, the devices and network connections that are inside a baseline envelope (the core area agreed by the Commission as to be under baseline control) taking into account the Licensee’s system design and the Licensee’s interface specification regarding a link to an external gaming system.

4.13.8 Approval for network connections from the baseline envelope to external gaming systems will be considered on a case by case basis taking into account the Licensee’s interface specification regarding a link to an external gaming system.

4.13.9 Approval for devices and network connections that are inside a baseline envelope will be subject to the principles established in Section 4.3.5.

4.13.10 Approval for information exchange with computer systems and terminals outside the baseline envelope will be considered on a case by case basis taking into account the principles established in Section 9.3.26.

5
Venue Requirements

This chapter sets out the requirements for the Licensee for operations carried out within Gaming Venues in Victoria.

5.1 General

5.1.1 Approval must be obtained from the Commission before placing into service any Monitoring Equipment, software or procedures which form an integral part of the approval.

5.1.2 Installation of Monitoring Equipment must conform to the requirements set down in Section 3.5.15 of the Act.

5.2 Responsibilities

Hardware and Infrastructure

5.2.1 It is the Licensee's responsibility to install and maintain all Venue CMCS Monitoring Equipment. This will include, at least:

i) Site Controllers;

ii) EGM interface devices;

iii) Jackpot Controllers, if the Venue elects to participate in jackpots;

iv) Jackpot display interfaces, if the Venue elects to participate in jackpots (excluding overhead signage, which is the Venue Operator's responsibility to provide, install and maintain);

v) Local area network for connecting the Venue CMCS to Gaming Equipment within a Venue;

vi) Wide area network for connecting the Venue CMCS to the Host CMCS;

vii) Venue Monitoring Equipment that is necessary in order to provide a real time link from the Venue CMCS to one or more gaming service providers and related external gaming system(s); and

viii) The locked cabinet that will house Venue Monitoring Equipment.

Operations

5.2.2 It is the Licensee's responsibility to:

i) Operate the Venue CMCS and manage its interfaces to the Venue equipment;

ii) Facilitate linked jackpots on behalf of the Venue Operator;

iii) Configure parameters for EGMs and jackpots on request of the Venue Operator; and

iv) Supply the Venue Operators with relevant manuals and instructions for using Licensee provided equipment within the Venue.

Venue Operators

5.2.3 Please refer to Appendix A, Section 15.1

5.3 Maintenance

5.3.1 Maintenance of Monitoring Equipment that is the responsibility of the Licensee is only to be conducted by an organisation(s) that is listed on the Roll of Manufacturers, Suppliers and Testers and is contracted by the Licensee.

Retention of Data

5.3.2 All Gaming Equipment statistics, Game Play information and metering information stored in the Gaming Equipment (whether by electronic, magnetic, mechanical or other means) or CMCS shall be retained during hardware maintenance and shall be protected against damage, destruction or alteration during maintenance operations (including battery replacement).

5.3.3 Maintenance procedures must be such that clearance of the metering information is only performed as a last resort if all other procedures have failed, and then may only be performed by procedures approved by the Commission.

Maintenance Not To Infringe Approval

5.3.4 Maintenance must be carried out in such a way that the Type Approval[11] for any equipment is preserved.

5.3.5 Maintenance or repair of Custom Built or Off The Shelf approved equipment must be undertaken using replacement parts that are identical or equivalent to the parts constituting an approved device

[11] Type approval is granted to a product that meets a minimum set of regulatory, technical and safety requirements.

and meets a minimum standard equivalent to the equipment submitted for approval.

5.3.6 Hardware maintenance of Monitoring Equipment shall not be by any of the following means:

i) Testing and fault diagnosis requiring the cutting of circuit board[12] tracks;

ii) Testing and fault diagnosis requiring the drilling of circuit boards;

iii) Testing and fault diagnosis requiring the addition of circuit board patch wires;

iv) Thermal overstressing of components; or

v) Removal or insertion of components while power is applied to the equipment, unless the equipment has been specifically designed to withstand such actions and then only by following the appropriate procedures laid down by the manufacturers.

5.3.7 All hardware maintenance will follow industry best-practice with respect to protecting the equipment from static discharge. In particular, where appropriate, the following shall be observed:

i) All components and assemblies must be stored and transported in anti-static packaging at all times;

ii) No components or assemblies are to be touched unless the technician is earthed via a wrist strap or other earthing device; and

iii) Maintenance work-areas must be earthed and fitted with earthed floor mats, earthed bench mats and wrist strap earth points.

5.4 Venue Keys and Locks

5.4.1 Keys and locks for the Monitoring Equipment in the Venues must offer a level of security that cannot be by-passed without leaving physical evidence of tampering.

Key Control

5.4.2 The Licensee must ensure that records are kept of all locks and keys supplied and these records must be available to the Commission request.

[12] A board, on which electronic components and their interconnecting circuits are mounted or etched.

5.5 Movement/Upgrade/Modification of Gaming Equipment/Monitoring Equipment

5.5.1 Hardware and software Revision Levels of each Gaming Equipment/Monitoring Equipment unit in the field must be tracked. As a minimum, records must be maintained for each device showing current Revision Levels of the Gaming Equipment/Monitoring Equipment, together with the corresponding unique Gaming Equipment/Monitoring Equipment identification information and current location and operational status of the Gaming Equipment/Monitoring Equipment.

5.6 Destruction of Monitoring Equipment

5.6.1 The Licensee must establish and maintain policies, standards and procedures, in accordance with the Act, relating to the destruction of Monitoring Equipment.

5.7 Venue Environment

5.7.1 The Licensee must provide a specification to Venue Operators for the Venue environment. This specification must cover at least:

i) Venue Electrostatic Discharge (ESD) protection;

ii) Venue environmental limits including a Venue’s:

a) Acceptable temperature and humidity range;

b) Power supply quality;

c) Power filters and conditioners; and

iii) Any other matters required by the Licensee and as agreed by the Commission.

6 Monitoring Equipment (Hardware)

This chapter sets out the hardware requirements for, primarily Venue based, Monitoring Equipment that must be followed for operation in Victoria.

6.1 Hardware Requirements

6.1.1 The design and configuration of all Monitoring Equipment Hardware and any changes to Monitoring Equipment Hardware must be submitted by the Licensee to the Commission for approval.

6.1.2 All hardware must meet the Hardware requirements set out in Section 2 of the National Standards and Section V2 of the Victorian Appendix to the National Standards.

Power Supply

6.1.3 Different units of Monitoring Equipment must be powered from separate sources. This is particularly important for communications interfaces to ensure continued monitoring during machine maintenance activities. That is, successive devices in the communications chain are to be powered from different sources.

Logic Area

6.1.4 The logic area is a locked cabinet area (with its own locked door) that houses electronic components that have the potential to significantly influence the operation of Gaming Equipment or Venue Monitoring Equipment.

6.1.5 Electronic components that are required to be housed in one or more logic areas are:

i) CPU's and other electronic components involved in the operation and calculation of jackpots;

ii) Electronics involved in the operation and calculation of jackpot result determination;

iii) Electronics involved in the maintenance of cash tickets;

iv) communication controller electronics and components housing the communication program storage media;

v) Interfaces and drivers for metering systems

vi) Purpose built device controllers (including Jackpot Controllers, disk and communications but excluding bank note acceptors, hopper interface boards, credit input mechanisms, card reader, Touch Screen, display boards);

vii) All jumper devices and tamper systems interfaces; and

viii) Any component that is involved in, or is capable of, influencing:

a) Game Play;

b) Signature computation or verification;

c) Computation or verification of any other check information;

d) Jackpot Play;

e) Random number generation;

f) Jackpot result determination;

g) Jackpot program storage;

h) Other writeable program storage;

i) Critical Memory storage;

j) Jackpot state and history;

k) Metering;

l) Significant events; or

m) Tamper monitoring.

Information Display

6.1.6 Commission approval must be obtained for the information that is to be displayed and the method of display of information, including jackpot outcome. The guidelines for such approval will be Victorian Legislation and Regulations and accepted community standards.

6.1.7 Displays must communicate with controlling devices via a protocol based form of communication.

6.1.8 “External” Displays employed in communicating the results of Games will be considered on a case-by-case basis by the Commission.

6.1.9 Video monitors, Touch Screens and printers used as information displays must meet the requirements set out in sections 2.4.33 to 2.4.39 of the National Standards.

6.2 Cash Input Systems

6.2.1 If cash input systems are to be used in Monitoring Equipment, the hardware requirements for these devices relative to credit input will be the same as for the Gaming Machines.

Card Reading Device

6.2.2 The Commission will consider the use of cards employing some form of electronic storage medium, for numerous purposes except credit betting which is prohibited under Section 3.5.31 of the Act.

Device I/O

6.2.3 Monitoring Equipment must protect against malfunctions, fraud or invalid results caused by the simultaneous or sequential activation of the various device inputs or outputs.

6.3 Cash Output Systems

6.3.1 If cash output systems are to be used in Monitoring Equipment, the hardware requirements for these devices relative to credit input will be the same as for Gaming Machines.

6.4 Jackpot Controllers

6.4.1 A Jackpot Controller may be a separate physical unit in the Gaming Machine (stand alone jackpots only), in the Venue or in the Licensee's central computer room. The Jackpot Controller may also be a 'logical' unit in the Gaming Machine, Site Controller or Host CMCS.

6.4.2 If a Jackpot Controller is not contained within the logic area of a Gaming Machine or Site Controller or in a secure computer room, then the security requirements which must be met are the same as for the logic area of a Gaming Machine, which includes tamper protection, signature checks, Significant Events and electrical interference.

Wiring Harness Interface to Jackpots

6.4.3 The Commission will not accept new Jackpot interfaces to EGMs where jackpot information is gathered via "wiring harness[13]" interfaces to the Gaming Machines, except where the EGM to be

[13] The cable (wiring) contained within an item of Gaming Equipment. Also used to indicate the method of collection of meters and events directly from the hardware outputs.

connected to the jackpot is unable to pass appropriate meter information in real time within the structure of the protocol.

7
Monitoring Equipment (Software)

This chapter sets out the Software requirements for Monitoring Equipment that must be followed for operation in Victoria.

7.1 Software Requirements

7.1.1 Commission approval must be obtained for the design and configuration of all Monitoring Equipment software and any changes to Monitoring Equipment software used within the CMCS.

7.1.2 All software must meet the software requirements set out in section 3 of the National Standards and Section V3 of the Victorian Appendix to the National Standards.

7.1.3 Some of the software requirements detailed in this section only apply to specific Monitoring Equipment. Following each section heading the applicable equipment for that software requirement will be listed. Where no equipment is listed the requirement is applicable to all equipment.

7.1.4 Some of the software requirements detailed in this section may not apply to specific Off The Shelf equipment where the Commission determines that the specific off-the-shelf equipment can operate in a manner acceptable to the Commission without the same level of requirements.

7.2 Software Functionality

Source Code

7.2.1 The source code for all software and Firmware components of the CMCS must be provided to the Commission and / or a Tester in an approved machine readable form. Program and functional documentation should also be provided.

7.2.2 Source code supplied to the Commission, and / or a Tester, shall be exactly as installed, programmed or loaded in the equipment to be used.

7.2.3 The following software identification must appear in all source code modules:

i) Module name;

ii) Revision Level;

iii) Brief description of functions performed; and

iv) Edit history; who, why and when (of changes made after this date).

Source Compilation

7.2.4 The Commission requires the ability to separately compile the CMCS program(s) to verify that the programs running are identical to the programs evaluated.

7.2.5 Software to be formally released to the live system, after approval has been received from the Commission, must have been generated (compiled) using the same process as for testing.

7.2.6 Should a manufacturer use an in-house, or proprietary development environment, the Commission will require submission of those tools for assessment.

Source Control and Upgrade

7.2.7 Separate approval must be obtained from the Commission for each software revision.

7.2.8 The Licensee must provide new versions of software organised by a software control system cross-referencing back to the previous release supplied to the Commission.

7.2.9 Software storage media must be clearly labelled, and the label must contain all software Version Control information. The identification used is at the discretion of the Licensee but it must strictly follow the Licensee’s identification system as detailed in the software change control procedures.

Software Functions Provided

7.2.10 All implemented functions must operate according to the intended design, all messages displayed must be true and accurate and the software must be free of unintended side effects.

Software Verification During Development

7.2.11 The Licensee and / or suppliers of gaming software must provide a method to the Commission to enable confidence to be gained that the software, on which evaluation was performed, system testing conducted and finally submitted for live operation are directly equivalent. To this end the following goals are to be met:

i) Source code must be provided (to the Commission or a Tester) in machine readable form for all components of the system deemed to be meaningful by the Commission;

ii) There must be a method available, to the Commission or its representatives, for examining the source code and conducting computer aided searches;

iii) There must be a method available, to the Commission or its representatives, for comparing two different versions of the source code and examining the differences between the two versions;

iv) There must be a method available of verification that the executable software that is to be used for testing has been compiled from the source code versions submitted to the Commission;

v) If software changes are required during the testing process, in accordance with the requirements at section 12, all changes must be submitted via the source code. Examination of differences and verification of executable or Data files will be undertaken by the Commission or its representatives by compiling the submitted source code;

vi) There must be a method available to verify that the executable software that has been used during the testing process is identical to that which is to operate on the live system. This verification procedure must occur when new software is installed, at the start of each trading day by the Licensee and randomly on demand by the Commission; and

vii) There must be a method available to determine if unapproved programs, command files, fixed Data files, etc. reside on any component in the gaming system. The method must have the ability to identify directories/files/records which contain variable Data and exclude them from verification.

7.2.12 Formal testing will not commence on any system if the first four steps are not in place. Live operation will not be approved until all steps are in place.

Memory Validation and Recovery

Storage of Information in Non Volatile Memory Devices

7.2.13 All dynamic configuration and “financial” information must be stored in critical Memory.

7.2.14 All such information stored must not be lost if there is a failure of a single component.

Critical Data Requirements

Only Applicable to:

- ***Site Controller***
- ***Communications Controller***
- ***Cashier Stations (dependent upon functionality implemented)***
- ***Jackpot Controllers***
- ***Peripheral Equipment***
- ***EGM Interface Card***
- ***EGM Protocol Converter***
- ***External Jackpot Display Interface (dependent upon configuration)***

7.2.15 Critical Memory constitutes Memory locations storing at least the following information:

i) Security events of Type R which have not been forwarded to the Host CMCS;

ii) Jackpot configuration;

iii) Jackpot Pools;

iv) Jackpot metering;

v) Cash tickets where maintained by the Monitoring Equipment;

vi) Unclaimed monies; and

vii) Any changeable configuration information.

7.2.16 The handling and maintenance of critical memory must meet the requirements of the National Standards 3.2.2 to 3.2.13.

Signatures

Only Applicable to:

- ***Site Controller***
- ***Communications Controller***
- ***Cashier Stations (dependent upon functionality implemented)***
- ***Jackpot Controllers***

- ***EGM Interface Card***
- ***EGM Protocol Converter***
- ***External Jackpot Display Interface (dependent upon configuration)***

Signature Computations Mandatory

7.2.17 Software signatures are to be calculated on all Gaming Devices at all Venues and are to be validated by “higher level” devices on the CMCS network.

Signature Algorithm Requirements

7.2.18 A signature algorithm must meet the following requirements:

i) It must combine all the contents of the software or Data being processed, (i.e. each and every bit of the contents must influence the signature result);

ii) It must combine the bits in a complicated and cross-interactive manner, based on the CRC method or equivalent as standard;

iii) Use of elementary techniques such as parity or simple “checksum” is inadequate and will not be acceptable;

iv) It must produce a result of at least 32 bits in width. The algorithm must detect at least 99.995% and preferably 99.998% of all possible Data errors;

v) The signature algorithm must be;

a) Fast and efficient; and

b) Able to process both individual software and fixed Data components and entire software suites.

Signature Seeding

7.2.19 Signature algorithm “Seeds” (or more generally “algorithm coefficients”) are to be supplied by the initiator of the signature request at the time of activation.

7.2.20 The following principles must apply to signature seeding:

i) The “seed” information must be at least 32 bits in length; and

ii) The “seed” information must influence the behaviour of the algorithm in a non-trivial way.

7.2.21 An example of unacceptable “seed” information would be, for a CRC algorithm, the initial value of the CRC register.

7.2.22 An example of acceptable “seed” information would be, again for a CRC algorithm, the initial address within the range of the item being checked at which the CRC calculation would commence, whilst the initial value of the CRC register may be a constant.

Signature Calculation Requirements

7.2.23 At a minimum a signature check must be completed over the entire Memory range of a device’s programs.

7.2.24 If the normal signature check of the said entire program exceeds 10 seconds, the Commission may approve a strategy of an immediate signature check of the “secure” parts of the program plus a background check of the entire program range when signatures are required. If this strategy is adopted, Commission approval must have been obtained for the separation of modules into the “secure” and “insecure” groups.

7.2.25 Signature checks are not required for program space that cannot be “interrogated” by the processor e.g. a character ROM.

7.2.26 Subject to the qualification of Section 7.2.25, the entire program PSD space, including unused areas, must be included in a signature calculation.

7.2.27 Files/records stored on Read/Write program storage media, which contain variable Data, are to be excluded from the signature calculation.

7.2.28 For CD-ROM and read/write program storage media, only the used program space should be included in the Memory signature calculation.

7.2.29 If CD-ROM and Read/Write program storage media also contain old approved versions of programs, the signature calculations initiated by the CMCS must only apply to the current operating version of the software on the storage media. A change or switch between versions must lead to a successful signature check on the newly activated program version.

7.2.30 If Flash Memory devices are used for Programmable Read Only Memory (PROM), where writing is external, the entire Memory area including the unused areas must be included in a signature calculation.

7.2.31 All methods of integrity check must have the ability to identify files/records which are variable Data and exclude them from the signature calculation.

7.2.32 A complete signature check is required for the entire range of the program, including fixed Data such as animations (excluding character ROM and space that cannot be interrogated), for a Gaming Device (e.g. local controller) when any of the following events happen:

i) Large jackpot win (as defined in the Jackpot Arrangement submitted for approval);

ii) The signature seed set is changed at the CMCS;

iii) New software is installed in the Gaming Device (i.e. a new PSD is installed or a download of new software has been actioned);

iv) Any power or communications failure of a Gaming Device;

v) A Memory reset has occurred;

vi) The logic door has been shut after being earlier opened; and

vii) A Gaming Device comes online which has never been online before.

7.2.33 The Commission may approve a background signature check[14] of the entire program range for devices which interface to multiple Gaming Machines.

7.2.34 If the background signature check fails, then the Gaming Device must be shut down immediately.

7.2.35 Where the software (including fixed Data tables) to be checked is held in multiple places, then signatures are to be computed for all instances of the software. Exemptions may be granted for this requirement where it can be demonstrated that the Version Control and security of the software is controlled by a method acceptable to the Commission. For example, it may be acceptable if all of the software is copied directly from one location to another (e.g. the entire program is copied from a disk to RAM - only the RAM copy shall need to be computed for the signature result). The following methods of must follow this principle (there may be others):

i) The software is stored on non-volatile storage device, but loaded into RAM for execution, (i.e. there is a storage instance on disk or EPROM and an operational instance in RAM). Note that this requirement does NOT apply to software held on disk that is paged in and out by the Operating System;

ii) The software is stored in a compressed form (e.g. on disk or EPROM), and expanded when loaded into RAM for execution, (i.e. again there is a storage instance on disk or EPROM and an operational instance in RAM); and

[14] A method of signature check, occurring with low priority, which allows normal operation of the device to continue (e.g. Gaming Machine Game Play).

iii) The software is downloaded and stored in multiple separate units of critical Memory, the multiple copies being used for comparison purposes to verify the correctness of the critical Memory contents.

7.2.36 It is recognised that in some of the cases defined above, e.g. (a) and (b), the signatures computed for each instance of the software may well be different. In such cases, the “total signature” becomes the concatenation of the signatures for each of the instances.

Venue Monitoring Equipment - Security

Only Applicable to:

- ***Site Controller***
- ***Communications Controller***
- ***Cashier Stations (dependent upon functionality implemented)***
- ***Jackpot Controllers***
- ***Peripheral Equipment***
- ***EGM Interface Card***
- ***EGM Protocol Converter***
- ***External Jackpot Display Interface (dependent upon configuration)***

Activities to be Inoperable when any Secure Cabinet Door is Open

7.2.37 Venue Monitoring Equipment must disable all player inputs and suspend all gaming functions while any of its doors are opened or remain open, unless maintenance tasks are being carried out.

De-activation when a Logic Area has been accessed

7.2.38 When a Venue Monitoring Equipment device determines that its restricted area has been accessed, the device must de-activate itself, and any Gaming Devices under its control, until appropriate investigations are conducted at which time the device shall only be re-activated by a method approved by the Commission.

7.2.39 When a Venue Monitoring Equipment device determines that a device under its control has had its restricted area accessed, the higher level device must de-activate that device until appropriate investigations are conducted at which time the device shall only be re-activated by a method approved by the Commission.

Tampering, Adjustment or Manipulation of Equipment

7.2.40 A random number generator (RNG), random selection process and jackpot result determination process must be impervious to influences from outside the device including but not limited to electrostatic interference[15], EMI/RFI interference and power supply interference.

7.2.41 There must be no way that a command can be received from a data communications line to alter the RNG.

7.2.42 Venue Monitoring Equipment must employ appropriate software means to protect the random number generator and random selection process from influence by associated equipment which is conducting data communications with the Gaming Equipment.

7.2.43 In order to prevent illegal tampering or manipulation that may affect Jackpot Play or outcome, or equipment operation, Venue Monitoring Equipment must not have any functions or parameters adjustable by or through any separate computer, input codes, application of ESD/EMI, dip switch, jumper or other software readable input device except for the following:

i) The adjustment of features that are wholly cosmetic (i.e. that do not affect functionality in any manner) as approved by the Commission;

ii) The download, in an authorised manner of any software, Data or operational parameter;

iii) An approved configuration (set-up) mode; and

iv) Other operational parameters as approved by the Commission.

Access to Restricted Features

7.2.44 Access to the following restricted features of Gaming Equipment shall be regulated by at least a key-operated switch, audit card, access to the inside of the equipment cabinet, password entry or other method to be approved by the Commission:

i) Auditing information[16];

ii) Metering information;

iii) Device configuration ;

iv) Test functions;

v) Cash ticket information;

vi) Jackpot information; and

vii) Any other features deemed to be restricted by the Commission.

[15] The physical property of being able to create electronic interference to a device by either discharging static electricity onto the surface of the unit (such as from a user), or via a mains power or communication cable (from lightning for example).

[16] The information required to be displayed by Communications and Jackpot Controllers that perform Self Audit Checks similar to Gaming Machines for their appropriate meters or meters received from Gaming Machines (refer section 3.3 of the National Standards).

Audible Alarm

Only Applicable to:

- ***Site Controller***
- ***Communications Controller***
- ***Cashier Stations (dependent upon functionality implemented)***
- ***Jackpot Controllers***
- ***Peripheral Equipment***
- ***EGM Interface Card***
- ***EGM Protocol Converter***
- ***External Jackpot Display Interface (dependent upon configuration)***

7.2.45 For Venue Monitoring Equipment accessible to the public, an audible alarm, or visual alarm viewable by appropriate personnel, must be provided by the Monitoring Equipment for signalling of door opens.

7.2.46 When the alarm is activated it must remain audible / visible for a minimum period of 1.5 seconds regardless of whether the alarm condition is cleared.

7.2.47 A logic door open event is to trigger such an alarm:

7.2.48 Accordingly, volume controls (either hardware or software set) for audible alarms must not be able to be adjusted to a level where the volume is barely audible. Volume controls secured in a logic area are exempted.

Recovery

7.2.49 In the event of a non-destructive fault or failure (e.g. power off), De-activation (e.g. disabled by host) or interruption (e.g. door opened), the Monitoring Equipment must be able to fully recover to its state immediately before the event, as soon as the condition is cleared and in accordance with the approved business continuity plan.

7.2.50 Monitoring Equipment must be able to recover in accordance with the approved disaster recovery plan and business continuity plan.

Program Memory Storage

7.2.51 The integrity of the operation of the device must be protected from nefarious or accidental use of the unused portions of the program Memory storage media (See sections 7.2.17 onwards for signature calculation requirements).

7.2.52 Specific requirements that apply to particular types of storage media are:

ROM Program Storage

7.2.53 All unused areas of ROM be written with the inverse of the erased state which for most EPROMs is zero bits (00 hex), rather than one bits (FF hex).

CD-ROM Program Storage

7.2.54 A CD-ROM used as a program or fixed Data storage device must be written such that only the actual program and Data required is written to the CD-ROM.

7.2.55 The operational software must provide an integrity check method to verify that there are no additional or missing programs or Data records/files on the CD-ROM.

7.2.56 There must be an ability to conduct an integrity check independent of the device's operational software to verify that there are no additional or missing programs or Data records/files on the CD-ROM.

7.2.57 Old approved versions of programs may be held on the CD-ROM. However, it must be possible to clearly identify which files belong to which version of the programs.

7.2.58 The method of changing to different versions of the program, including reversion to old versions must be submitted to the Commission for approval.

Read/Write Storage Media

7.2.59 A Read/Write Storage device used for storage of program or Data must be written in such a way that only the actual program, Data and the system control and configuration files that are necessary and sufficient to meet the application functionality required by the program utilising the storage device is written to the storage device.

7.2.60 The operational software must provide an integrity check method to verify that there are no additional or missing programs or fixed Data records/files on the storage device.

7.2.61 There must be an ability to conduct an integrity check independent of the device's operational software to verify that there are no additional or missing programs or Data records/files on the storage device.

7.2.62 All methods of integrity check must have the ability to identify directories/files/records which are variable Data and exclude them from the signature calculation.

7.2.63 Commission approval must be obtained for the method of loading programs to the storage media.

7.2.64 Old approved versions of programs may be held on the storage media. However, it must be possible to clearly identify which files belong to which version of the programs.

7.2.65 Commission approval must be obtained for the method of changing to different versions of the program, including reversion to old versions.

Flash Memory Devices - Downloading Programs

7.2.66 Commission approval must be obtained for the method of loading programs to the Flash Memory device.

7.2.67 Only the actual program, Data and system control and configuration files that are required are to be written to the Flash Memory device.

Flash Memory Devices - Program Verification

7.2.68 During the programming operation on Flash Memory, each byte programmed must be verified by a method that is proven to work and is acceptable to the Commission.

Setup - Device Configuration

Only Applicable to:

- ***Site Controller***
- ***Communications Controller***
- ***Cashier Stations (dependent upon functionality implemented)***
- ***Displays***
- ***Jackpot Controllers***
- ***Peripheral Equipment***
- ***EGM Interface Card***
- ***EGM Protocol Converter***
- ***External Jackpot Display Interface (dependent upon configuration)***

7.2.69 A variable required to be set during device configuration or set-up must be able to be set only once per valid Memory clear or able to be changed by a secure method approved by the Commission.

7.2.70 A Gaming Device must not be able to be operated unless all configuration variables are set.

7.2.71 A device may be configured remotely or by direct access via an approved mechanism.

7.2.72 If Memory becomes corrupted, a Gaming Device must not assume default values and re-commence gaming operation unless the assumed values have been configured by an approved mechanism.

Prescribed Formats for Date and Time Display or Printing

7.2.73 See National Standards 3.3.25 to 3.3.27.

7.2.74 [redacted] Blank.

Cash Input / Output Device Control

7.2.75 If cash input / output devices are to be used in Monitoring Equipment, the software requirements for these devices relative to credit input will be the same as for the Gaming Machines.

Card Reading

7.2.76 If cards employing a form of electronic storage of Data are to be utilised, the Commission would have to be satisfied with all aspects of security. Some of the major concerns are:

i) Prevention of illegal alteration of Data;

ii) Protection from loss of Data;

iii) Recovery of information from damaged or lost cards;

iv) Accuracy of read/write operations; and

v) Protection from fraudulent duplication of card information.

7.2.77 Where cards are used for Account Betting[17], no bet will be permitted to exceed the balance of an account.

Information Display

Printer

7.2.78 Where a printer is provided, software must interpret sensor outputs to determine if one of the following events has occurred:

i) Paper out/low; and

ii) Printer disconnection or power loss.

Cash-Out by Printed Ticket

Only Applicable to:

- ***Site Controller***
- ***Communications Controller***
- ***Cashier Stations (dependent upon functionality implemented)***
- ***Jackpot Controllers***

[17] Bets placed against an account that has had credit/money deposited into the account before gaming takes place.

- ***Peripheral Equipment***
- ***EGM Interface Card***
- ***EGM Protocol Converter***
- ***External Jackpot Display Interface (dependent upon configuration)***

7.2.79 See National Standards 3.7.12 to 3.7.14.

7.2.80 Where a payout is by ticket voucher printed by the Monitoring Equipment, the Monitoring Equipment must be capable of printing a ticket voucher for all credits owed.

7.2.81 A cash ticket request must be rejected by the Venue CMCS if the device that generates the cash ticket serial number is conducting a signature check or is de-activated except in the instance where the device is off-line to the Host CMCS.

Touch Screens

7.2.82 See National Standards 3.8.12 to 3.8.16.

Clock

Requirement for Clock

7.2.83 All devices that perform any of the functions listed in Section 7.2.86 must maintain an internal clock that reflects the date and 'Standard Time' in Victoria. 'Standard Time', as defined in Part 3 of the Justice Legislation (Amendment) Act 2005, is time that is 10 hours in advance of Co-ordinated Universal Time[18].

7.2.84 Standard Time, as referred to in 7.2.83, is only applicable during non daylight savings time periods. During daylight savings time periods, internal clocks should reflect the time that is 11 hours in advance of Co-ordinated Universal Time.

7.2.85 Time for the clock must be maintained to accuracy to the nearest second.

Uses of Clock

7.2.86 The clock must be used for the following purposes:

i) Time stamping of Significant Events;

ii) Time stamping of player transactions such as credit transfer to/from a Gaming Machine or jackpot wins;

iii) Time stamping of configuration changes; and

[18] Co-ordinated Universal Time is a time standard based on International Atomic Time and is determined by the International Bureau of Weights and Measures (http://www.bipm.org/en/scientific/tai/time_server.html).

iv) Cash ticket transactions.

Update of Clock by CMCS

7.2.87 The CMCS must be able to update its internal clock(s) and those of all devices in the system (e.g. Gaming Machines, Site Controllers, and Jackpot Controllers) in at least the following circumstances:

i) Manual request by the Licensee. Manual intervention must be audit logged;

ii) Transition to/from daylight savings time; and

iii) Determination of inaccurate clocks in devices in the system.

Automatic Update of Inaccurate Clocks

7.2.88 Each device must have a method of determination of inaccuracy of its clock and an automatic method of re-synchronising the time from a higher level device in the CMCS. A Significant Event must be created whenever a resynchronisation is performed.

7.2.89 Determination of the inaccuracy of the clock must be:

i) By the device itself - from time information periodically passed from the CMCS; and

ii) By a CMCS higher level device - from time information periodically passed from the device (e.g. Gaming Machine forwards current clock to the Venue CMCS on every idle poll).

De-Activation of Gaming Equipment by the CMCS

Only Applicable to:

- ***Site Controller***
- ***Communications Controller***
- ***Cashier Stations (dependent upon functionality implemented)***
- ***Jackpot Controllers***
- ***Peripheral Equipment***
- ***EGM Interface Card***
- ***EGM Protocol Converter***
- ***External Jackpot Display Interface (dependent upon configuration)***

7.2.90 The following point relates to issues associated with De-activation of Gaming Equipment which may occur as a result of:

i) Gaming Equipment malfunction; and

ii) Gaming Equipment De-activation (self initiated or from a higher level device of the Monitoring Equipment).

Consequence of De-Activation

7.2.91 Monitoring Equipment must suspend all gaming functions, in a controlled and auditable manner, while Gaming Equipment is de-activated.

Activation of Gaming Equipment by the CMCS

Only Applicable to:

- ***Site Controller***
- ***Communications Controller***
- ***Cashier Stations (dependent upon functionality implemented)***
- ***Jackpot Controllers***
- ***Peripheral Equipment***
- ***EGM Interface Card***
- ***EGM Protocol Converter***
- ***External Jackpot Display Interface (dependent upon configuration)***

New Gaming Equipment

7.2.92 Gaming Equipment that is new in operation, as far as the CMCS is concerned, must be treated as if the logic cage had been opened; that is a signature check must be conducted and verified by the CMCS.

7.2.93 The Host CMCS must not enable any Gaming Equipment that maintains meters until a successful poll of the meters of the Gaming Equipment is received and sent to the Host CMCS.

Licensed Hours

7.2.94 The CMCS must maintain a record of the liquor license hours for each Venue.

7.2.95 The liquor license hours can be variable over the period of operation with a number of special cases and the CMCS must cater for this variability.

7.2.96 Gaming Equipment, including new Gaming Equipment, must not be activated for Game Play outside the Venue's licensed hours.

i) The CMCS must disable Gaming Equipment, for Game Play, at the end of the current day's liquor license hours for that site; and

ii) The CMCS must not enable Gaming Equipment for a site before the commencement of the liquor license hours.

7.2.97 Gaming Equipment, including new Gaming Equipment, may be activated for testing purposes outside the Venue's licensed hours if prior approval has been obtained by the Venue Operator and the Licensee from the Commission.

Re-Activation of Gaming Equipment

7.2.98 In general, after Gaming Equipment has been de-activated, the method of activating the Gaming Equipment requires manual intervention by the Venue Operator or Licensee, as appropriate. The following exceptions apply:

i) If a door open event occurs, other than a logic door open, the Gaming Equipment may automatically re-activate when the door is closed;

ii) If the power fails on Gaming Equipment, De-activation occurs as a matter of course. After power is restored, the CMCS must initiate a signature check of the Gaming Device. Once the Gaming Device is advised by the system of the passing of the signature check, it is permitted for the Gaming Equipment to automatically re-activate itself unless it determines that the logic door(s) has been opened while the power was down, in which case the Gaming Equipment must remain de-activated until manually re-activated, and only after the Commission audit procedures are satisfied. (The Venue Operator may choose to require manual Re-activation in all cases if desired.);

iii) If Gaming Equipment detects a communications failure, De-activation must occur immediately after the Down_Time_Permitted period. Once communications are restored, the CMCS must initiate a signature check of the Gaming Device. Once the Gaming Device is advised by the system of the passing of the signature check, it is permitted for the Gaming Equipment to automatically re-activate itself unless it determines that the logic door(s) has been opened while the communications were down, in which case the Gaming Equipment must remain de-activated until manually re-activated, and only after the Commission audit procedures are satisfied. (The Venue Operator may choose to require manual Re-activation in all cases if desired.);

iv) If Gaming Equipment is automatically de-activated at the end of the Venue's Gaming Day it is permissible for the CMCS to automatically re-activate the Gaming Equipment when the next permitted session commences; and

v) If the PIN retry limit is exceeded for a player's account, the Gaming Equipment must remain de-activated until the card is removed.

7.3 Metering

Meter Overflow

Only Applicable to:

- ***Site Controller***
- ***Communications Controller***
- ***Cashier Stations (dependent upon functionality implemented)***
- ***Host CMCS***
- ***Jackpot Controllers***
- ***Peripheral Equipment***
- ***EGM Interface Card***
- ***EGM Protocol Converter***
- ***External Jackpot Display Interface (dependent upon configuration)***

7.3.1 The Meter Width must be such that a meter must not wrap more than once in any one day, and in any case shall be at least seven digits in dollars.

7.3.2 Venue CMCS meters must be able to accommodate and maintain a record of meter wrap occurring on a Gaming Device.

7.3.3 In the event that a meter, of any type, reaches its maximum value it must automatically wrap back to zero and subsequently continue counting (from zero) in the normal way.

Meter Integrity

7.3.4 No software shall have a mechanism by which an error will cause a meter, of any type, to clear or to assume any other incorrect value.

Self Audit Error Checking

Only Applicable to:

- ***Site Controller***
- ***Communications Controller***
- ***Cashier Stations (dependent upon functionality implemented)***
- ***Jackpot Controllers***
- ***Peripheral Equipment***
- ***EGM Interface Card***
- ***EGM Protocol Converter***
- ***External Jackpot Display Interface (dependent upon configuration)***

Other Venue Devices Self Audit Check

7.3.5 Site Controllers or their slaves and Jackpot Controllers must perform Self Audit Checks similar to Gaming Machines for their appropriate meters or meters received from Gaming Machines.

7.3.6 The cases of a 'meter roll-over' must be taken into account when performing a "Self Audit" check.

Occurrence of Self Audit Check

7.3.7 In addition to the above ,the Site Controller must perform the Self Audit Check at least at the following times:

i) During start up; and

ii) At the start and the end of every jackpot.

7.3.8 The EGM Interface Card must perform the self audit check at least at the following times:

i) During start up;

ii) Before EGM Interface Card communication with the EGM is recovered; and

iii) Every time the EGM Interface card detects change to EGM meter values.

Action on Failure of Self Audit Check

7.3.9 A CMCS Device must enter an unrecoverable memory corruption state in the event that this Self Audit Check fails.

7.3.10 The CMCS must De-activate a Gaming Device if it detects the Gaming Device has failed a Self Audit Check.

Cash Clearance Procedures

Only Applicable to:

- ***Site Controller***
- ***Communications Controller***
- ***Cashier Stations (dependent upon functionality implemented)***
- ***Central Monitoring and Control***
- ***Jackpot Controllers***
- ***Peripheral Equipment***
- ***EGM Interface Card***
- ***EGM Protocol Converter***
- ***External Jackpot Display Interface (dependent upon configuration)***

7.3.11 The Gaming Equipment and CMCS must display the appropriate meter information, supporting the cash clearance. The accounting information must be available both for the entire period of operation of the Gaming Equipment (since the last Memory reset) and since the last Cash (Coin or Note) Clearance.

7.4 Central Control versus Standalone Operation

Standalone Gaming Machines not Permitted

7.4.1 Any installed machine must, at all times it is in operational mode, where valid Game Play is possible, be in on-line communication with the Venue CMCS.

7.4.2 This means specifically:

i) For an EGM, when it loses communications with the next point of the Venue CMCS for a period longer than twenty (20) seconds, the Gaming Machine must disable itself;

ii) For an EGM Interface Card when it loses communications with the next point of the Venue CMCS for a period longer than 20 seconds, the EGM Interface Card must disable its Gaming Machine;

iii) For Site and Communication Controllers, when it loses communications with the Host CMCS for a period longer than Down_Time_Permitted, the Monitoring Equipment must disable all Gaming Machines and jackpots attached to it; and

iv) Down_Time_Permitted mentioned in the previous point must be a system parameter that can be extended / shortened but only after approval has been granted by the Commission. The default value of Down_Time_Permitted is one (1) Gaming Day. This parameter is to be interpreted as meaning at the end of the next Gaming Day for that Venue.

7.4.3 There must be a means to extract meter and event information from Site and Communications Controllers after such a period to enable further operation of the site, i.e. the Down_Time_Permitted counter to be reset after the information is extracted.

Jackpot EGMs Offline

7.4.4 If the EGM is offline to its Jackpot Controller (local or central) for a period of 20 seconds or more, the EGM must be treated as per Section 8.1.5 including disabled if relevant.

8 Jackpots: Control and Display

This chapter sets out jackpot requirements that must be followed for operation in Victoria. For further reference an overview of Jackpots can be found in Appendix C.

8.1 Jackpot Handling

8.1.1 The following principles apply to the implementation of all types of jackpots, though many are appropriate to “linked jackpots”. The requirements for each individual style of jackpot are in the subsequent sections.

8.1.2 Jackpot handling is not limited to Venue Monitoring Equipment, since Jackpot System implementation may be integrated into both the Venue CMCS and the Host CMCS systems.

Jackpot Fairness

8.1.3 In progressive linked style jackpots (Game outcome), if a jackpot requires a certain minimum bet level in order to participate in the jackpot, then:

i) The player must be made clearly aware of this situation;

ii) There is a clearly indicated prize, which is paid to the player if the jackpot trigger combination is achieved but the minimum bet level is not; and

iii) The base Game Return to Player (RTP), including the effect of this prize, must theoretically operate above the return to player proportion as defined in Section 3.6.1 of the Act.

8.1.4 In order to have a jackpot that is equally fair to all players the following principles must apply:

i) All players that play jackpot Games must be eligible to win the jackpot. Exceptions to this jackpot rule must be submitted to the Commission for individual approval before any development work on the jackpot is commenced;

ii) Jackpot contributions must not be assimilated into revenue;

iii) If a cap is established on any jackpot, all additional contributions once that cap is reached are to be credited to a

Diversion Pool;

iv) In mystery linked style jackpots, the probability of the player winning the jackpot must be directly proportional to the size of the bet, unless the expected base Game Player return (sum of non-jackpot prizes) for Gaming Machines that participate in Jackpots is greater than or equal to the return to player proportion as defined in section 3.6.1 of the Act.

v) The proportionality factor in part (iv) must not vary between type of Gaming Machine and/or Game(s) played;

vi) The proportionality factor in part (iv) must not be achieved by modification of the method of selection or determination of the Game result; and

vii) The progressive win must be based upon a random event.

Jackpot Shutdown / Re-activation

8.1.5 A jackpot shutdown should occur in the following instances:

i) The Venue's gaming hours have expired.

a) Note: a wide area Jackpot may be able to continue in other sites;

ii) A door open on the Jackpot Controller;

iii) A signature failure on the Jackpot Controller;

iv) A signature failure on the Site Controller;

v) A logic cage open on the Site Controller;

vi) An internal fault in the Jackpot Controller;

vii) No relevant jackpot displays are operational;

viii) Communications to the Jackpot Controller are offline, e.g. the Host CMCS is the Jackpot Controller and the link from the site to the Host CMCS is down or the link to the Site Controller from the Jackpot Controller within a site is down;

ix) The communication link to the Site Controller from the Jackpot Controller within a Venue is down;

x) A jackpot has been eliminated or suspended; or

xi) A Venue CMCS based Jackpot Controller is unable to send its meters to the Host CMCS for a period longer than 30 hours.

8.1.6 The Licensee may have the ability to manually command a jackpot shutdown.

8.1.7 A jackpot shutdown requires the following action:

i) Clear indication must be given to players that the jackpot is not operating (e.g. by saying "Jackpot Closed" on LED displays).

ii) It must not be possible for the jackpot to be won while in the shutdown state;

iii) If the expected player return for non-jackpot prizes on Gaming Machines that participate in this jackpot is less than the players' proportion prescribed in the Act, or any determination under the Act, these Gaming Machines must be de-activated from Game Play until the jackpot is re-activated.

iv) If the expected player return for non-jackpot prizes on Gaming Machines that participate in this jackpot is greater than the players' proportion prescribed in the Act, or any determination under the Act, but the jackpot win determination is by Game result, these Gaming Machines must be de-activated from Game Play until the jackpot is re-activated unless there is a default prize that is awarded should the jackpot triggers occur as per Section 8.1.3 (ii); and

v) Any jackpot shutdown or Re-activation must lead to all of the EGMs in the jackpot, which are not de-activated, to have their PID accurately reflect the appropriate player return at that time and situation.

8.1.8 Re-activation of the jackpot from the shutdown state must return the jackpot with the identical parameters, including jackpot value and increment percentages, as before the shutdown.

8.1.9 On Re-activation for mystery jackpots, hidden win amounts may be recalculated in the range of current jackpot value and maximum jackpot amount. The calculation must pick a new number in the range of the current (recovered) amount and the maximum.

Jackpot Update and Display

Requirement for Jackpot Displays

8.1.10 If the information normally displayed on a Jackpot Display including jackpot win notification is also displayed on all participating Gaming Machines, then this shall be considered to be a 'Jackpot Display'.

8.1.11 If each individual bet is not to be passed to the Jackpot Controller, the local computers or controllers must accumulate jackpot increments and forward them frequently and accurately to the Jackpot Controller. Commission approval must be obtained for this period.

8.1.12 Jackpot Displays must have the capability to display the current amount of the jackpot(s), which must be updated accurately and as often as possible so as to reasonably reflect the current size of the prize pool. When a jackpot prize is won then the display must "catch up" to the precise value of the jackpot won.

8.1.13 If no jackpot display capability is operating at a Venue (i.e. all methods of displaying the current jackpot amount to participants of the jackpot have stopped operating) the jackpot must be shutdown at the Venue as per Section 8.1.5.

8.1.14 Jackpot Displays must show the latest win of the jackpot(s) including amount won and the winning Gaming Machine number in an unambiguous format for a defined period. Commissionapproval must be obtained for this period.

8.1.15 If the status of the jackpot is not discernible on the Gaming Machine, at least one jackpot display must be visible to each player who plays that jackpot Game.

8.1.16 If a minimum Jackpot is advertised, the Jackpot Display must never display an amount less than the minimum jackpot.

8.1.17 If a maximum Jackpot is advertised, the Jackpot Display must never display an amount greater than the maximum jackpot.

8.1.18 The Jackpot Display must never display an amount greater than the current value of the jackpot.

8.1.19 The jackpot Display must never stop incrementing when active Game Play is in progress.

8.1.20 The Jackpot Display must not be more than ten seconds behind the current jackpot amount.

8.1.21 If more than one win occurs for a jackpot at approximately the same time, all such jackpots wins must be shown on the jackpot display. It is not acceptable to overwrite the first win with the second without a reasonable display period. Commission approval must be obtained for this period.

Jackpot Win Notification and Reset

8.1.22 The following indications of the winning of a jackpot prize are required:

i) Audible;

ii) Visual indication of such an event on the winning Gaming Machine;

iii) Visual indication of the win on the main Jackpot Display, unless all the information on the display is available on all the participating Gaming Machines; and

iv) Significant Event sent to the CMCS.

8.1.23 The notification of the winning of any jackpot must be passed by electronic means to the winning Gaming Machine which must signify in an approved manner to the player that they have won the jackpot and the amount that they have won.

8.1.24 Commission approval must be obtained for the method by which the player receives the jackpot payment.

8.1.25 The method of “Resetting” the jackpot display so as to no longer show the last win details must be secure and approval obtained from the Commission. An example of a reset method that would be approved is a special “jackpot reset key” at the Jackpot Controller.

8.1.26 When a Jackpot is reset, a Significant Event must be sent to the CMCS.

Mystery Jackpot Winner Selection

8.1.27 Mystery jackpot winner selection must use a random number process which meets the full requirements of Sections 3.14.1 to 3.14.15 of the National Standards.

8.1.28 Mystery jackpot wins must only occur when the player who wins the mystery jackpot is still at the Gaming Machine which is to win the jackpot. To achieve this goal:

i) Mystery jackpot wins must be notified to the winning Gaming Machine before the end of the Game Play which triggered the win; and

ii) The mystery jackpot win notification, or similar messages approved by the Commission, must be received by the winning Gaming Machine within three seconds of the commencement of the Game.

8.1.29 Game Play conducted on a Gaming Machine in the period before, during and after a restart of the Jackpot Controller or other component of the CMCS must be properly handled. This handling is to include, but not be limited by:

i) Game Play conducted on a Gaming Machine in the period before a restart of the Jackpot Controller or, other component of the CMCS which was used in the jackpot winner selection process, must be fully recovered to the same state before recommencing the Game Play;

ii) Game Play conducted while the Gaming Machine is offline to the Jackpot Controller or the Host CMCS is down must not lead to a mystery jackpot win in itself when the connection to the Jackpot Controller is re-established or the Host CMCS restarts. The Licensee, and also the Venue Operator, must make a proposal satisfactory to the Commission as to the handling of such offline Game Play; and

iii) If handling of contributions from offline involves placing them in the current or subsequent jackpot(s), the Licensee, and also the Venue Operator, must specify how it will handle the circumstance where the contributions would make the jackpot at or near the jackpot maximum.

Jackpot Special Cases

8.1.30 The CMCS must be able to properly handle and account for the following Gaming Machine special cases:

i) Gaming Machine critical Memory reset;

ii) Gaming Machine removal from the jackpot;

iii) Gaming Machine removal from the system;

iv) Gaming Machine meter rollover;

v) Gaming Machine meter audit check failure; and

vi) Abnormal meter jumps / discontinuities.

8.1.31 The CMCS must be able to properly handle and account for a Critical Memory reset of a Jackpot Controller.

8.1.32 The CMCS must be able to properly handle and account for a meter Self Audit Check failure of a Jackpot Controller.

Multiple Jackpot Winners

8.1.33 The Licensee, and also the Venue Operator, must submit to the Commission for approval its proposal for dealing with the possibility of a jackpot being won (or appearing to be won) by one or more players at approximately the same time i.e. within a minimum time window.

8.1.34 The minimum time window (Jackpot Reset Period) is not less than the longest time taken to:

i) Register that a jackpot has been won;

ii) Announce the win on the display;

iii) Lock up the winning Gaming Machine(s); and

iv) Reset the progressive meters.

8.1.35 Resolution of this problem is required and rules, documented procedures and notice to patrons must be submitted and approval obtained from the Commission before the jackpot is implemented.

Linked Jackpot Winners When Communications Go Down

8.1.36 It is necessary to resolve the problem that occurs when a Gaming Machine or controller determines that a jackpot has been won, but the link to the main Jackpot Controller becomes inoperable.

8.1.37 Resolution of this problem is required and rules, documented procedures and notice to patrons must be submitted and approval obtained from the Commission before the jackpot is implemented.

8.1.38 Commission approval must be obtained, by the Licensee, and also the Venue Operator, for the method of determining the jackpot amount.

8.1.39 Should there be implemented a “manual” method of entry of a jackpot win on the Host CMCS, or Venue CMCS, the Commission will need to be assured that there are no security risks with the entry of manual jackpot win events by verification of the procedures for making a manual entry. Commission approval must be obtained for any manual method of entry.

Signature Checking and Jackpots

8.1.40 A signature check must be conducted, before formally awarding a prize, on a Gaming Machine which has won a Game determined progressive jackpot with a win greater than $10,000.

8.1.41 A signature check must be conducted, before formally awarding a prize, on a Jackpot Controller which has declared a mystery jackpot win greater than $10,000.

Jackpot Design

8.1.42 The design of the Jackpot System must consider ways that testing can be conducted of the extreme jackpot circumstances, including but not limited to:

i) Win level values right at the top;

ii) Win levels right at the bottom; and

iii) High values in the reserve pool.

Jackpot Communications

Protocol

8.1.43 There must be a reliable communications protocol, as defined in Section 9 between Jackpot Displays and Jackpot Controllers.

8.1.44 Cryptographic Data Security, encryption and/or message authentication is required on Critical Data communicated between Jackpot Controllers and Gaming Machines in linked multi-Venue jackpot configurations. Refer to Section 9.2.

8.1.45 Except as otherwise approved, communication of jackpot information (i.e. jackpot increments and win notification) between the Gaming Machine and the external Jackpot Controller, or CMCS, must be via protocol-based communication with the computer that controls the Gaming Machine. The method of communication and protocol to be used must be submitted to the Commission for approval.

8.1.46 A Jackpot Controller must monitor increment values from Gaming Machines to ensure they are within an approved tolerance. If they are not within the approved tolerance:

i) The invalid Data must be ignored;

ii) A Significant Event must be forwarded to and recorded by the CMCS; and

iii) The Gaming Machine providing the invalid Data must have its progressive Game(s) disabled.

Master/Slave Jackpot Controllers

8.1.47 Where a “Master Controller” employs “Slave Controllers” to control a Jackpot the following requirements apply:

i) Communication between masters and slaves must meet all of the communication requirements as for Gaming Machines, Site Controllers and Jackpot Controllers;

ii) All Slave Controllers must be time synchronised with the Master Controller;

iii) The Master Controller must be time synchronised with the CMCS;

iv) Game-result Jackpot Win events must be time-stamped and the Jackpot Controller must ensure that wins registered within a minimum time increment are considered as simultaneous wins. Prize payout for simultaneous wins are to be made in accordance with Sections 8.1.33 - 8.1.35; and

v) If supporting a Mystery Jackpot, the processing of receipt of increments from all Gaming Machines whether on a Master Controller or a Slave Controller must be fair.

Transmission of Jackpot Meter Information to CMCS

8.1.48 The Jackpot Meter Information must be periodically transferred from the Jackpot Controller to the Host CMCS and recorded there. Commission approval must be obtained for this period.

8.1.49 If a Jackpot Controller has not sent its meter information to the Host CMCS for a period exceeding 30 hours, it must de-activate itself as per Section 8.1.5.

8.2 Jackpot Parameters

Changes

8.2.1 Unless permission is received from the Commission for a Jackpot Conversion as per Section 8.2.19, once a Jackpot has commenced, parameter changes must not take effect immediately – rather they must be saved to apply after that Jackpot is next won. These are 'pending' parameters.

8.2.2 The pending Jackpot must have a parameter to flag that it will be applied after the active jackpot is won.

8.2.3 The active Jackpot must have a parameter to flag that it is to be modified or closed when the jackpot is next won.

8.2.4 The system must provide a means of displaying current and pending jackpot parameters.

Partial Jackpot Redirection

8.2.5 The Commission may grant approval to the implementation of a Diversion Pool scheme by taking a portion of the jackpot contributions and redirecting them to another pool so that when the current jackpot is won, this pool is added to the restart level of the next jackpot. Variable diversion rates might apply depending upon the size of the current jackpot. (Care must be taken in the design to ensure that the diversion pool does not grow to infinity. The Commission will not approve a jackpot redirection scheme where the mathematical expectation of the diversion pool is infinite).

8.2.6 The Commission may approve a Jackpot scheme whereby the Diversion Pool is used to fund a “minimum or start-up level”. However, in these circumstances the minimum jackpot amount is deemed to be zero for the purposes of calculation of expected player return.

8.2.7 Venue based jackpots may access and increment a common reserve pool for the Venue for increasing the start-up value of the next jackpot after a win, or each jackpot must have its own reserve pool. Commission approval must be obtained for the rules for the transfer of moneys from a common reserve pool to finance the next jackpots after a jackpot is won.

8.2.8 A Wide-area Jackpot may utilise a reserve pool but common reserve pools are not allowed for multiple Wide-area Jackpots.

8.2.9 Diversion pools must not be capped.

Parameters

Limit of Maximum Prize

8.2.10 The Commission may limit maximum prizes for each jackpot implementation. Factors to be assessed by the Commission for approval of jackpot prizes will include, but not be limited by the following:

i) The jackpot implementation is game determined or mystery;

ii) The Commission is satisfied that the trigger value of a mystery jackpot is stored in a location and format that cannot be interrogated;

iii) The payment of the jackpot to the patron is preceded by a successful signature check of the Gaming Machine, and Jackpot Controller reconciliation between the software meters of all participating Gaming Machines and the increment of the jackpot amount and diversion pools (if any);

iv) There is a system provided method of identification of winners of jackpots, e.g. personalised player card or the Venue Operator ensures all participating Gaming Machines are video monitored and recorded (with play back capacity of a minimum of 48 hours). The standard of video monitoring must be sufficient to allow these checks; and

v) Pre-payment procedures involve a review of recorded activity on the Gaming Machine (including identification of the winning patron).

Note: The Commission may also impose significant win procedures in addition to these controls.

Fixed Prize Jackpots

8.2.11 Please Refer to Appendix A, Section 15.3

Jackpot Approval

Approval Required

8.2.12 All jackpots, including relevant jackpot parameters (as defined in Section 8.2.14) and jackpot participation (as defined in Section 8.2.15), must be submitted for approval by the Licensee, in association with the Venue Operator, to the Commission. No jackpot shall operate without prior approval for its parameters granted by the Commission.

Sets of Jackpot Parameters

8.2.13 Multiple sets of jackpot parameters may be submitted to the Commission for approval.

Parameters to be Approved

8.2.14 Commission approval must be obtained for the values of the following Jackpot parameters, for each level of the jackpot scheme, both for the initial operation of a jackpot or for subsequent modification:

i) Jackpot Minimum(s) - the base or reset amount(s) and how it is funded, if any;

ii) Jackpot Maximum(s) and what happens to excess contributions, if any;

iii) Jackpot Contribution Rates as a percentage of the amount bet;

iv) Diversion Pool Percentages, if any; and

v) The probability of winning the jackpot level where the result is Game determined.

Jackpot participation

8.2.15 Jackpot submissions must indicate the Venue(s) and which EGMs in each Venue that is to participate in the jackpot.

Multi-site Mystery Jackpots

8.2.16 Multi-site mystery jackpots are to provide equity for players. The following specific rules must apply:

i) The probability of any Venue winning such a jackpot must be directly proportional to the Venue’s contributions to the jackpot;

ii) Venues which operate with longer operational hours must have no greater chance of winning the jackpot other than that gained by increased contributions that shall apply to that Venue due to the longer hours;

iii) Fairness for new Venues, Venues with increased or decreased Gaming Machine numbers or Venues that have had their operation suspended for a period must be catered for in any jackpot scheme; and

iv) Within a Venue, the probability of any Gaming Machine winning such a jackpot must be directly proportional to the level of play on the Gaming Machine.

Jackpot Parameter Storage

8.2.17 Current jackpot amounts must be stored in absolute amounts (in units which have been approved the Commission), rather than in terms of numbers of plays of the jackpot. This will also facilitate the conversion of a jackpot Gaming Machine from one denomination to another.

8.2.18 The Commission will not approve the conversion of Gaming Machine jackpot denominations unless this requirement is met.

Conversion of Jackpots

8.2.19 The Licensee, in association with the Venue Operator, must receive permission from the Commission if one or more jackpot pools are to be converted or combined into other jackpot pool(s) in accordance with the approval for that jackpot.

8.2.20 If the effect of the conversion is to alter the effective player return for the jackpot component, the Player Information Display (PID) must be updated for all participating EGMs for the new jackpot parameters.

8.2.21 If the jackpot(s) conversion leads to an overflow of jackpot contributions, the overflow must be paid into a diversion pool and added over time to subsequent Jackpot Pools via a method that will require approval by the Commission.

8.2.22 A Mystery Jackpot, which uses a hidden jackpot amount to determine the jackpot win, must re-calculate the hidden jackpot amount, as per Section iii), when an active Jackpot is converted (i.e. had any jackpot contributions added to it) unless the new parameters are inconsistent with the current jackpot amount.

Elimination of Jackpots

8.2.23 The Licensee, in association with the Venue Operator, must receive permission from the Commission if a Jackpot Pool is to be eliminated.

8.2.24 If a Venue-based jackpot is discontinued, the accrual amount of the jackpot (and any diversion or reserve pools specific to that link) must be paid to an escrow pool and treated as per Section 8.2.21 or subtracted from the escrow pool if a negative figure.

8.2.25 If the Venue is ceasing all jackpots or is closing, the total of all Jackpot Pool Accruals for that Venue must be added to the net cash balance (or subtracted if a negative figure) provided that:

i) A Venue must not (by making this adjustment) be in breach of Section 3.6.1 (Returns to players) of the Act; and

ii) A Venue if continuing to conduct gaming shall only terminate a jackpot immediately after the jackpot is won.

8.2.26 If a Venue ceases to participate in a wide area jackpot, the increment from Gaming Machines at the Venue remains part of the prize pool and must be available to be won as prizes on machines that remain linked to the jackpot.

8.2.27 If a wide area jackpot is discontinued, the accrual amount of the jackpot (and any diversion or reserve pools specific to that link) must be paid to an escrow pool and treated as per Section 8.2.21.

8.2.28 If a wide area jackpot scheme is ceasing all jackpots, the Jackpot Pool Accruals for each Venue participating in the jackpot schemes are to be added to the Venue's net cash balance (or subtracted if a negative figure).

8.3 Jackpot Meters and Accounting

Software Meters

8.3.1 The following software meters, as a minimum, must be stored and maintained:

i) Total amount played for jackpots;

ii) Total amount of jackpots won;

iii) Total jackpot contributions made, (includes any diverted a mounts);

iv) Total jackpot contributions won;

v) Current amount for each jackpot;

vi) Current diversion pool for each jackpot, if any;

vii) Number of times the logic area(s) have been accessed; and

viii) Current value of Jackpot contributions diverted.

8.3.2 The Host CMCS must record the values of all jackpot meters for EGMs and Jackpot Controllers.

8.3.3 For each Jackpot Controller the following Data must be held, stored and reported by the Host CMCS:

i) Jackpot contributions made for the last Gaming Day; and

ii) Jackpot contributions won for the last Gaming Day.

Accounting

8.3.4 As Victoria, for taxation purposes, utilises net cash balance which allows for jackpot contributions to be totally deductible, linked

Jackpot Systems must provide adequate reconciliation to ensure that all jackpot contributions deducted:

i) Have been won by players as prizes; or

ii) Are held in accountable reserves (which can be demonstrated) to be paid to players in the future, (i.e. as part of future prizes); or

iii) Are properly dispersed in case of elimination of jackpots as per Sections 8.2.23 - 8.2.28.

8.3.5 Accounting reconciliations are to be performed at least daily by the Licensee at the Venue level for Venue level jackpots, and at wide area level for wide area jackpots. These reconciliations must be provided to the Venue Operator as required.

8.3.6 The electronically collected Data from the Gaming Machines and Jackpot Controller are to be submitted to allow the Commission to perform independent reconciliations. Commission approval of the form of the submitted Data must have been previously received.

8.3.7 A Gaming Machine may participate in both single Venue and Wide-area Jackpots provided that the accounting of the Venue based and Wide-area Jackpots is separately maintained in the Gaming Machine, Jackpot Controllers and Host CMCS.

8.3.8 If the Gaming Machine controls the jackpot and does not pass full Game Play information to the Venue CMCS as each Game is played, then the above statistics must be included with other required accounting information.

8.3.9 As referred to in other parts of these specifications, a Gaming Machine must not permit itself to enter Game Play if it has not passed its normal and jackpot accounting statistics to the Host CMCS within the last 30 hours.

Retention of Jackpot Monies

8.3.10 Commission approval must be obtained for the procedures for the collection and payment of Jackpot contributions and payments.

Jackpot Recovery

8.3.11 To enable recovery of the current value of the Progressive Jackpot amount(s) in the case of a Gaming Machine (for stand alone jackpots) or Jackpot Controller failure, either:

i) The current value of the progressive amount must be stored in at least one other physically separate device from the controller, (it is not sufficient to rely on the amount displayed unless it can be shown that a controller failure would not corrupt the amount displayed at the time of failure); or

ii) The current value of the progressive amount is able to be accurately calculated from other metering information.

Standalone Progressive Recovery Procedures

8.3.12 For Gaming Machines with Standalone Progressives[19], should there be a total Gaming Machine and/or critical Memory failure, it will be necessary to recover the “un-won” jackpot contributions into the replacement Gaming Machine. However, the Commission views the ability to “Manually Change” a jackpot amount as a potential security risk. The Licensee, in association with the Venue Operator, must specify a method of handling this recovery situation, approval of which must be obtained from the CCommission.

[19] A jackpot feature contained within a single EGM. Only that EGM contributes to the prize and the prize can only be won on that EGM.

9
Network and Communications

This chapter sets out network and communications requirements that must be followed for operation in Victoria.

9.1 Communications Requirements

Communication Scheme

9.1.1 Unless otherwise agreed by the Commission:

i) All communications must be via a protocol based communications scheme;

ii) Signature verification of all Venue equipment software must be initiated and the outcome verified by a separate, higher level component of the CMCS; and

iii) The system must have the ability to send messages to a device to disable/enable all gaming operations on that device.

On-Line Real Time Communications

9.1.2 Game Play on a Gaming Machine must only occur when the Venue CMCS is in direct communication with that Gaming Machine, and its operations are in compliance with the requirements of Section 7.4.

Communication Ports

9.1.3 See National Standards 2.7.1 to 2.7.2.

Line Isolation

9.1.4 To achieve mains power static discharge immunity from lightning, and other (including deliberate) static discharges, Monitoring Equipment communication interfaces must have at least 3 kV of line isolation. This requirement shall override any manufacturer’s communication specifications.

9.1.5 Rationale: This requirement protects Monitoring Equipment against lightning strikes and interference to Monitoring Equipment via the communication lines.

9.1.6 Gaming Machines or other devices are not to interfere with each other via the attached communication lines.

Electromagnetic Interference

9.1.7 When subjected to human body or any other source of electrostatic discharges, a CMCS component must not severely interfere with any other connected CMCS component.

Power Disruption

9.1.8 If the supply of mains power to a Gaming Device (or any other equipment in the Venue connected in any way to any Gaming Equipment or Monitoring Equipment) is disrupted, the device must not interfere with the operation of any other attached device (e.g. via local data communications cabling).

Ground Isolation

9.1.9 There must be no mains ground interconnections via data cabling between devices powered from different supply circuits unless adequate line isolation is in place.

9.1.10 Note that RS-232-C[20] must be used only if the two communicating devices are powered from the same supply circuit and the cable length between the two devices is acceptable to the Commission.

Telecommunications Requirements

9.1.11 All telecommunications conductors, if any, leaving premises must be fitted with gas discharge protection components, or similar devices, which provide at least the same protection, at the premise's telecommunications main distribution panel. The use of isolation transformers is not sufficient.

Data Communications

Protocol

9.1.12 Commission approval must be received in advance for any protocol used for data communications between Gaming Devices.

9.1.13 The assessment will also extend to the adequacy of documentation which is to be distributed to selected suppliers for interfacing with the system operating the chosen protocol.

[20] A set of EIA standards specifying various electrical and mechanical characteristics for interfaces between computers, terminals, and modems. The standard applies to both synchronous and asynchronous binary data transmission at rates below 64 kbps.

9.1.14 The Commission will only approve a protocol if it is confident that the devices implementing the protocol will fully comply with the requirements of the Victorian Technical Standards.

Data Link

9.1.15 Communications protocols must include the following:

i) Error Control;

ii) Flow Control; and

iii) Link Control (remote connection).

Error Detection

9.1.16 Communications protocols must make use of Cyclic Redundancy Checks (CRC's) or the equivalent - use of only parity or simple checksum byte is not acceptable.

9.1.17 Communications protocols must be able to withstand varying error rates from low to high. Data communication error generators shall be used by a Tester to verify this.

Data Communication Control of Gaming Machines

9.1.18 The CMCS must ensure only approved control functions of Gaming Devices be implemented. These control functions must be clearly specified in any relevant EGM protocol or communication protocol documentation.

Communications Failure Modes and Recovery

9.1.19 All Monitoring Equipment must be able to "gracefully" handle a range of simple failures.

9.1.20 Some typical tests which may be implemented by the Commission or its representatives to test compliance with the VCR are:

i) Failure of central computer LAN interfaces;

ii) Failure / jam of central LAN;

iii) Failure of central data communication interface devices;

iv) Failure of single data communication interface;

v) NTU failure at central;

vi) NTU failure at remote;

vii) High data communications error rates on line;

viii) A foreign or additional device placed on a LAN;

ix) A foreign or additional device placed between LAN bridges, communications controllers, or on data communication lines between sites;

x) Single data communication port failure on remote controller (if any);

xi) LAN failure on Regional or Local Controller (if any);

xii) LAN failure on Cashier Terminal (if any); and

xiii) Data communication interface failure on a Gaming Machine.

9.1.21 Hosts attached to broadcast networks must recover from broadcast storms that flood the network to 100% utilisation for a period of up to 30 minutes without losing any critical information.

9.2 Cryptographic Data Security

Introduction

9.2.1 Cryptographic Data Security refers to the protection of critical communication data from eavesdropping and/or illicit alteration.

9.2.2 Eavesdropping protection is achieved by using an approved encryption algorithm.

9.2.3 Protection against illicit alteration is achieved by using an approved message authentication code algorithm although some encryption algorithms also provide this protection.

Requirement for Cryptographic Data Security

9.2.4 Except, as approved on a case by case basis, the following requirements related to Cryptographic Data Security apply:

i) Cryptographic Data Security must apply to all Critical Data that traverse data communications lines. This does not apply to communications within a single logic area;

ii) Cryptographic Data Security must apply for all Critical Data communication transfer between all Venue equipment, and between a Venue and the Central Site (but not necessarily within the Central Site), except as approved on a case by case basis;

iii) Examples of Critical Data security which would be satisfied by an approved encryption algorithm include:

a) RNG seeds;

b) Signature seeds (algorithm coefficients);

c) Signature results;

d) Encryption keys, where the implementation chosen requires transmission of keys;

e) PINs; and

f) Passwords.

iv) Examples of Critical Data security which would be satisfied by an approved message authentication algorithm include:

a) Software uploads and downloads of any security related software (e.g. signature, RNG);

b) Transfers of money, including unclaimed money, to/from player accounts;

c) Transfer of money, including unclaimed money, between Gaming Equipment; and

d) Jackpot meters, parameters, configuration, win messages.

v) There must be a password protected and secure function to disable encryption to handle circumstances where difficulty with communications is encountered. Disabling of encryption must only occur with the prior approval of the Commission.

Encryption Algorithm Approval

9.2.5 Commission approval must be obtained for the encryption algorithm, its implementation and operational procedures pertaining. The following are encryption characteristics that will be considered:

i) Encryption algorithms are to be demonstrably secure against cryptanalytic attacks;

ii) The minimum width (size) for encryption keys is 112 bits;

iii) There must be a secure method implemented for changing the current encryption key set; and

iv) It is not acceptable to only use the current key set to “encrypt” the next set. An example of an acceptable method of exchanging keys is the use of public key encryption techniques to transfer new key sets.

Message Authentication Algorithm Approval

9.2.6 Commission approval must be obtained for the message authentication code algorithm, its implementation and operational procedures pertaining. The following are authentication characteristics that will be considered:

i) Message authentication code algorithms are to be demonstrably secure against cryptanalytic attacks;

ii) Message authentication code algorithms are to be designed such that it is feasibly impossible to take a hash value and recreate the original message, “impossible” in this context means “cannot be done in any reasonable amount of time.”; and

iii) Message authentication code algorithms are to be designed such that it is feasibly impossible to find two messages that hash to the same hash value.

Encryption Keys

9.2.7 Commission approval must be obtained for the key algorithms to be used to provide Cryptographic Data Security which must conform to industry standard encryption and authentication structures.

9.3 Network Requirements

General

9.3.1 This section describes the Commission’s expected minimum network requirements on system Firewalls and network connections that are inside a baseline envelope (the core area agreed by the Commission as to be under baseline control) and network connections from the baseline envelope to external devices. The Commission will determine exact requirements dependent upon the Licensee’s system design.

Network Baseline

9.3.2 During the approval stage of a system network, and based on the System Baseline Document prepared by the Licensee, the Commission will determine the core areas of the system network that it will maintain verification control over and this will be defined and approved in a Network Policy Document. This document is the responsibility of the Licensee to prepare as part of its submission to the Commission when obtaining approval for the CMCS. This document must describe the network topology of the system detailing the interconnection of modules within the network and the types of connection between the modules that is permitted.

Physical Requirements

9.3.3 Power to devices inside and on the boundary of the baseline envelope must be provided from a filtered, dedicated power circuit. As a minimum standard, this requirement applies to any Monitoring Equipment that is capable of affecting the outcome of a Game on a Gaming Machine, a jackpot arrangement, or a significant Game Play transaction.

9.3.4 Cabling used in production networks must be protected against unauthorised physical access and malicious damage.

Network Documentation

9.3.5 All cabling and devices must be clearly labelled by function.

9.3.6 Network documentation must be kept on site and at the disaster recovery site in a form that can be viewed in the event of total network destruction. Documentation must include patch records, device configuration, device location, cable location and fault procedures.

Connection of Devices to Networks Inside a Baseline Envelope

9.3.7 Unused ports on network devices and network control devices inside and on the boundary of the baseline envelope are to be disabled. This provision applies equally to Venue and Central Site networks.

9.3.8 Host computer systems, network devices and network control devices inside and on the boundary of the baseline envelope must be immune from high loads (e.g. broadcast storms) or faults on any part of the network outside the baseline envelope.

9.3.9 Configuration changes to all devices inside and on the boundary of the baseline envelope must be password protected. Password protection procedures must exist and be implemented. This provision applies equally to Venue and Central Site networks.

9.3.10 An audit log must be maintained for all changes to the configuration of any network devices inside and on the boundary of the baseline envelope. The audit trail must not be modifiable by persons authorised to make the configuration changes.

9.3.11 At a Central Site, all network devices, network control devices and hosts associated with a production network must be located inside an area that only authorised people can enter.

Communications Within a Baseline Envelope

9.3.12 Hosts within the same baseline envelope must be able to communicate when the sustained utilisation of any and all networks within the envelope is 50%.

9.3.13 Hosts within the same baseline envelope must be able to communicate when the sustained bit error rate of any and all networks within the envelope is 10^{-6} for Local Area Networks, and 10^{-5} for Wide Area Networks.

9.3.14 There must be no loss of information due to a failure of a redundant communications network within a baseline envelope.

Communications between Separate Baseline Envelopes

9.3.15 Critical information flowing between different baseline envelopes must be subject to authentication and encryption, unless the intervening network is physically secure and under the complete control of the Licensee. Note that WAN communication links will be generally deemed to be outside a baseline envelope.

9.3.16 Hosts in separate baseline envelopes that communicate with each other must be able to communicate when the sustained utilisation of any and all networks between the envelopes is 50%.

9.3.17 Hosts in separate baseline envelopes that communicate with each other must be able to communicate when the sustained bit error rate of any and all networks between the envelopes is 10^{-6} for Local Area Networks and 10^{-5} for Wide Area Networks.

9.3.18 There must be no loss of information due to a failure of a redundant communications network between baseline envelopes.

9.3.19 Communication between devices in separate baseline envelopes must be immune from “man-in-the-middle” attacks.

Communications to Devices Outside a Baseline Envelope (Firewall)

9.3.20 Data exchanged with computer systems and terminals outside the baseline envelope must pass through at least one network control device (e.g. router or Firewall). The network control devices must implement the controls as defined in the Network Policy Document, which must be prepared by the Licensee and submitted to the Commission for approval.

9.3.21 The network control devices involved in implementing the Network Policy Document must be located at the boundary or inside the baseline envelope.

9.3.22 An audit log must be maintained for all changes to the configuration of any network control devices inside and on the boundary of the baseline envelope. The audit trail must not be modifiable by persons authorised to make the configuration changes.

9.3.23 Network control devices must be configured to discard all traffic other than that which is specifically permitted by the Network Policy Document. Configurations that discard specific traffic types and allow everything else are not acceptable.

9.3.24 Computer Systems within the baseline envelope must not be affected by network attacks emanating from outside the baseline envelope (e.g. ping-of-death attacks, teardrop attacks, routing protocol attacks, etc.).

9.3.25 Operational procedures for network control devices must include the capturing and regular review and follow-up of all access violations.

9.3.26 Approval for information exchange with computer systems and terminals outside the envelope will be considered on a case by case basis taking into account the following:

i) Authentication scheme;

ii) Encryption scheme. Encryption must occur at the boundary and inside the baseline envelope;

iii) Physical security of the external terminal devices and computer systems;

iv) Host level security of the external terminal devices and computer systems;

v) Physical security of the network (including intervening hubs, bridges, routers, etc.) to the external devices;

vi) The sensitivity of the information being transferred;

vii) Whether the computer system inside the baseline envelope or outside the baseline envelope initiates information transfer;

viii) Audit information recorded on the CMCS pertaining to the transfer (date, time, person account or system account, and file(s) transferred);

ix) Immunity from man-in-the-middle attacks; and

x) Note: The WAN communication links will be generally deemed to be outside the Commission envelope.

Host Monitoring Systems and Network Management Systems

9.3.27 Commission approval must be obtained for host monitoring systems that monitor hosts inside or on the boundary of a baseline envelope.

9.3.28 Commission approval must be obtained for network monitoring systems that monitor network devices and network control devices inside or on the boundary of a baseline envelope.

9.3.29 The configuration of host monitoring systems and network management systems must not be changed without approval from the Commission. Automatic verification of the configuration of these systems must be performed at least daily.

9.3.30 A device outside a baseline envelope must not be able to affect the configuration of network devices or network control devices within the Host CMCS and its related facilities, by:

i) Imitating the IP address of a host monitoring system or a network management system; or

ii) Imitating the hardware address (e.g. Ethernet address) of a host monitoring system or a network management system; or

iii) Replaying previously captured communications.

9.3.31 A device outside a baseline envelope must not be able to affect the operation of a central monitoring host and must not be able to read or modify Critical Data by:

i) Imitating the IP address of a host monitoring system or a network management system; or

ii) Imitating the hardware address (e.g. Ethernet address) of a host monitoring system or a network management system; or

iii) Replaying previously captured communications.

Verification tools

9.3.32 The Commission must be provided with sufficient tools and/or procedures to verify the configuration of all devices inside and on the boundary of the Commission envelope.

9.4 Wireless Communication

9.4.1 Wireless communication may be acceptable to the Commission provided that there are appropriate additional security measures in place, which meet the standards set out for wireless communication in the Australian Government Information and Communications Technology Security Manual (ISM)[21], to overcome the general weaknesses of wireless communication,

9.4.2 Wireless communication will be considered for Local Area Network communications within Venues and/or Wide Area Network communication between Venues and the Host CMCS.

9.4.3 The wireless access point must be physically positioned so that it is not easily accessible by unauthorised individuals.

9.4.4 The access point must not be placed directly onto the Venue network unless a stand-alone stateful packet inspection Firewall is employed.

9.4.5 Wireless network traffic must be secured with additional encryption and/or authentication codes and must meet the requirements of Section 9.2.

9.4.6 The keys used to encrypt the communication through the wireless network must be stored in a secure location.

[21] http://www.dsd.gov.au/library/infosec/ism.html

9.4.7 In addition to security aspects, the Commission will consider performance and availability before granting approval to the use of wireless communication.

10
CMCS Significant Events

This chapter sets out CMCS Significant Events requirements that must be followed for operation in Victoria.

10.1 General

10.1.1 This section is a summary of each of the CMCS Significant Events that are required, including the type of event.

10.1.2 The following list defines four (4) types of Significant Event and the "type" numbers used elsewhere refer to this list:

TYPE 1 Information only (no De-activation).

TYPE 2 Events that lead to automatic De-activation but also allow for immediate automatic Re-activation when the condition is cleared (e.g. authorised door open).

TYPE 3 Events that lead to automatic De-activation and require manual Re-activation.

TYPE 4 Events that lead to automatic De-activation and require manual Re-activation, but only after the Commission audit procedures are satisfied. These procedures must involve immediate approval for Re-activation, or the approval is withheld until physical inspection by a Commission Inspector is completed.

10.1.3 Also with some events is a suffix:

"R" Means that the event must be reported by the Host CMCS in the daily "Type 4 Events Report". Note that some events with this description are not Type 4 Events. By definition, all Type 4 Events are reportable.

10.1.4 It should be noted that the Commission monitors Significant Events at its premises and that each of the Significant Events will be tested during the formal acceptance tests.

10.2 Significant Events

Events Determined by the CMCS

10.2.1 The following are the Significant Events relative to Gaming Machines that are determined by the CMCS. The subsidiary points in the system must also detect and forward the events and force De-activation where required:

Software Security Breach

10.2.2 Opening of a logic door in a cabinet containing software {Type 4,R}: All Gaming Machines under control of the element of the CMCS that has had the door opened must be de-activated and must not be automatically re-activated. (In the case of Gaming Machines or local controllers a “Logic Area Access” event is sufficient).

Note: This requirement only applies to Monitoring Equipment outside of a secure computer room.

Signature Failure

10.2.3 Modification of Game software {Type 4, R}: the system must be able to detect that a Gaming Machine’s software has changed by failure of a signature, (whether foreground or background), and/or version test.

10.2.4 Loading of Gaming Machine software not approved by the Commission {Type 4, R}: the determination of this error shall be by signature and/or version check failure.

10.2.5 The failure of either of these tests is a most important Significant Event and must lead to De-activation of the Gaming Machines and Jackpots controlled by the Monitoring Equipment. Re-activation must not be actioned until the signature failure is resolved and the Licensee manually re-enables it.

Gaming Machine Off line

10.2.6 Failure of a Gaming Machine to be on-line {Type 1, R}: this does not lead to Venue CMCS initiated De-activation of a Gaming Machine (because it is not on line anyway) but is a most important Significant Event. The system must report all instances of Gaming Machines that were expected to be on-line but are not. This must be implemented as a reporting requirement - every day the CMCS must generate an electronic media report of all Gaming Machines reported as being off-line and with zero financial transactions for the previous day as a Gaming Machine may be on-line all day but experience no transactions.

Gaming Machine Online in Incorrect Venue

10.2.7 Coming on line of a Gaming Machine in the wrong Venue. {Type 4, R}: the system must ensure that a Gaming Machine cannot be on line other than its approved Venue.

Unauthorised PIN

10.2.8 Incorrect PIN three times consecutively with a machine card {Type 3} & player card {Type 1}: The system must ensure that the Gaming Machine remains de-activated until the card is removed.

Unauthorised Card

10.2.9 Use of a stolen or unauthorised machine card & player card {Type 3}: It is mandatory that the Gaming Machine card reader, if it has a card locking mechanism, try to hold onto the illicit card, or card not authorised for use at this time, until manually cleared in some manner by an authorised person.

Controller

Controller Fault

10.2.10 {Type 3, R}: All Gaming Machines and jackpots that are controlled by these devices are to be de-activated until the problem is rectified.

Jackpot Events

Jackpot Display Fault/Disconnect

10.2.11 {Type 2, R}: When all displays for a jackpot have failed, all jackpots including progressive Games are to be de-activated until the problem is rectified.

Progressive Award

10.2.12 {Type 3, R}: Any progressive jackpot that is declared by Gaming Equipment or Monitoring Equipment must be logged by this Significant Event. It must indicate which Gaming Machine(s) won the jackpot and the amount of the award.

Bonus Award

10.2.13 {Type 3, R}: Any bonus award that is declared by Gaming Equipment or Monitoring Equipment must be logged by this Significant Event. It must indicate which Gaming Machine(s) won the bonus(es) and the amount of the award.

Jackpot Parameter Change

10.2.14 Creation or deletion of a jackpot or modification to a jackpot's parameters {Type 1, R}: the following Data must be included with this Significant Event:

i) Jackpot minimum(s);

ii) Jackpot maximum(s);

iii) Jackpot contribution rate(s);

iv) Diversion pool limit(s); and

v) Current jackpot amount(s) (if the jackpot is deleted).

Jackpot Device Configuration Change

10.2.15 Addition of deletion of Venue and / or EGMs participation in a jackpot. {Type 1, R}: the following Data must be included with this Significant Event:

i) Venue(s) added;

ii) Venue(s) deleted;

iii) EGM(s) added; and

iv) EGM(s) deleted.

Jackpot Reset

10.2.16 {Type 1, R} Refer to Section 8.1.26.

Invalid Gaming Machine Increment

10.2.17 {Type 4, R} Refer to Section 8.1.46.

Miscellaneous Events

Time Clock Re-synchronisation

10.2.18 {Type 1, R} Refer to Section 7.2.88.

11
Submission Requirements

This chapter sets out the submission requirements for evaluation in Victoria. It primarily applies to the Licensee's Monitoring System and Monitoring Equipment.

11.1 General

11.1.1 The submission to the Commission for approval, at the minimum, must include the following:

i) Background of the CMCS;

ii) Purpose of the submission

iii) Description of the scope of system and operational changes;

iv) Tester recommendation of the CMCS in accordance with above requirements;

v) The Licensee's comments on any conditions included in the Tester recommendation;

vi) List of all software versions and associated CRCs;

vii) List of all relevant hardware and operating systems – product names, models and versions;

viii) Associated systems that are connected to the CMCS;

ix) A CMCS Baseline Document; and

x) A Network Policy Document.

11.2 CMCS/Site Operator Requirements

Procedural & Environment

11.2.1 The Commission must be satisfied that all procedures pertaining to the requirements of Section 5, Venue Requirements have been addressed. To this end, the Licensee must have internal controls, rules and procedures manuals or other documents as applicable which are consistent with this document and other Commission requirements. These documents must be available for assessment by the Commission.

Communication Requirements

11.2.2 Provide all protocol documents.

Line isolation and EMI/ESD Immunity

11.2.3 The Licensee must supply the following information for each communications interface:

i) Technical means by which line isolation is achieved;

ii) Line isolation voltage achieved; and

iii) Data communications

Simulation Software

11.2.4 Provide simulation software to enable simulation of all commands and manipulation of all message types between device and controller. This requirement applies to all communications between physically distinct devices. For example:

i) Gaming Machine to Jackpot Controller;

ii) Jackpot Controller to Host CMCS;

iii) Communications controller to Host CMCS;

iv) Gaming Machine to Site Controller; and

v) Others.

Protocols

11.2.5 Descriptions of all protocols and message formats are to be supplied.

i) Gaming Machine ‹—› Site Controller. (Note: Site Controller includes site communications controller);

ii) Site Controller ‹—› Regional controller. (regional controller includes front end processor);

iii) Regional controller ‹—› Host CMCS;

iv) Host CMCS ‹—› other systems (e.g. Commission's computer systems);

v) Cashier terminal ‹—› Venue CMCS;

vi) Gaming Machine ‹—› peripheral equipment; and

vii) Venue equipment ‹—› external gaming systems.

11.2.6 Descriptions of the physical interfaces of these various data communication links are to be provided, in particular, including details with respect to insertion of data communication error generating equipment, protocol emulation, protocol testing and protocol monitoring devices.

Cryptographic Data Security

11.2.7 The following information must be provided relative to Cryptographic Data Security algorithm(s):

i) Description of the algorithm(s);

ii) Theoretical basis of the algorithm(s);

iii) Results of any analyses or tests to demonstrate that the algorithm(s) is suitable for the intended application;

iv) Rules for selection of keys, if appropriate; and

v) Means of setting and protecting keys, if appropriate.

11.2.8 Information must be supplied to explain the situations during which data encryption and message authentication will be employed.

Communications Transmission Medium and Method of Device Connection

11.2.9 Provide details on communication transmission medium and device connection.

Local Area Network (LAN)

11.2.10 LANs (e.g. multi-dropped terminals, Ethernet) typically provide relatively little in terms of protection against the insertion of “rogue devices” on the LAN. Provide details of the means of security to prevent illegal access in the following events:

i) PC or other device inserted on a LAN; and

ii) PC or other device inserted on an unused LAN port of a local or Jackpot Controller.

Electronic Monitoring System Requirements

CMCS Architecture

11.2.11 Provide an overview of the system design.

11.2.12 Provide a functional specification of the system.

11.2.13 Provide detailed design documents (including but not limited to data flow diagrams, data dictionaries, etc.).

11.2.14 Provide details of the CMCS covering areas such as:

i) Duplication strategy;

ii) Disk Subsystem;

iii) Magnetic back-up facilities;

iv) Printing;

v) Operating system;

vi) Power requirements; and

vii) Air conditioning requirements.

11.2.15 The information requested above in ‘CMCS’ applies also to other Monitoring Equipment to be used in the Host CMCS environment. This must include such devices as appropriate:

i) Front ends;

ii) Remote controllers;

iii) Multiplexing equipment;

iv) Switching equipment;

v) Routers; and

vi) Repeaters.

Central Logging

11.2.16 Describe where and how information is stored throughout the system.

11.2.17 Identify what statistics are stored by the system for each separate Gaming Equipment type.

Device Configuration Database

11.2.18 Indicate how the requirements for the verification of system application software is realised.

Banknote Input Support

11.2.19 Provide details of the support for Banknote input meters provided by the Gaming Machine interface protocol.

11.2.20 Provide details of the support for Banknote specific Significant Events provided by the Gaming Machine interface protocol.

11.2.21 Provide details of how Money In totals are derived and maintained by the system including any banknote input specific meters.

11.2.22 Provide details of support for banknote deposit into CMCS maintained accounts.

Retention of Unclaimed Moneys

11.2.23 Describe the register of unclaimed prize monies and how it is maintained.

11.2.24 Describe the treatment of revenue from expired, uncashed tickets.

Password Protection

11.2.25 Describe in detail the password protection systems and associated algorithms utilised by the system.

Transaction Logging

11.2.26 Describe the method of transaction logging used.

Encryption of Stored Data

11.2.27 The following information must be provided:

i) Description of the algorithm;

ii) Theoretical basis of the algorithm;

iii) Results of any analyses or tests to demonstrate that the algorithm is suitable for the intended application;

iv) Rules for selection of keys; and

v) Means of setting and protecting keys.

11.2.28 Information must be supplied to explain the situations during which encryption of data files will be employed.

PIN Management

11.2.29 The following information must be provided.

i) Description of the PIN creation algorithm;

ii) Theoretical basis of the algorithm; and

iii) Results of any analyses or tests to demonstrate that the algorithm is suitable for the intended application.

11.2.30 Information must be supplied to explain the implementation of PIN creation.

CMCS Hardware

11.2.31 Provide details on the hardware configuration of the CMCS, providing a functional description of each module.

User Interface, Documentation and Reporting

11.2.32 Provide Operator’s Manuals.

11.2.33 Provide copies of all standard reports produced by the system and describe how these are generated.

11.2.34 Provide System Administrator Manuals.

11.2.35 Provide Operator’s Procedures Manuals.

Link to Commission Computing Facilities

11.2.36 Provide details on the manner in which it is proposed this facility is provided.

11.2.37 Detail any special procedures to be followed when using the facility.

11.2.38 Details are to be provided of the hardware, software and data communications facilities that will be available to support this link.

11.2.39 Provide details of the online access of Commission staff to the Licensee’s system.

Test System

11.2.40 Access to the Licensee’s integration test (“dummy live”) environment must be provided. This must include load simulators together with quantities (sufficient for load testing) of all varieties of Gaming Equipment and Monitoring Equipment, all configured and functioning in a full live and operational manner.

Submitted Equipment

11.2.41 The equipment under test must have operating software during the tests and the effects if any on the correct functioning of the software is assessed as part of the tests.

11.2.42 The equipment that is submitted for testing must be a production standard model and must be in “normal operation” during the test, including communication with a CMCS or approved simulator (where the equipment employs some form of data communications).

Site Requirements

11.2.43 Provide documentation that describes the minimum standards that are to be met by each site. This documentation must include electrical wiring, data communication wiring, cabinetry and/or structural modifications (if any), environmental specifications, Telstra installation (if any), Electrostatic Discharge (ESD), etc.

12
Testing Requirements

This chapter sets out the CMCS testing requirements that must be followed for operation in Victoria.

12.1 Inspection and Testing

12.1.1 The Commission may have regard to a recommendation for system approval from a Tester listed on the Roll of Manufacturers, Suppliers and Testers as defined in the Act.

12.1.2 The Licensee must establish and maintain policies, procedures and standards for quality assurance[22] and control equivalent to ISO9000, and a test strategy that includes consideration of the need to test:

i) Network hardware and communications infrastructure;

ii) System functionality;

iii) System interfaces;

iv) Usability, including ease of use for customer facing devices and Graphical User Interfaces (GUI);

v) Accessibility, including consideration of World Wide Web Consortium (W3C)[23] standards, or equivalent;

vi) User acceptance;

vii) Performance, including consideration of load generation for response, stress, volume and soak testing of system, database and network configurations;

viii) Security, including consideration of testing system and network configurations for vulnerability, penetration, hacking, cracking, virus, spy ware, spam or denial-of-service attacks;

ix) Disaster recovery;

x) Business processes; and

xi) Business readiness, including provision for a live trial when required by the Commission.

[22] The methods an organisation puts in place to ensure reliable quality control.

[23] An international community where member organisations, full-time staff, and the public work together to develop Web standards. (www.w3.org)

12.1.3 The Licensee's test strategy must identify any independent or third party testing, including internal and external test facilities, and the engagement mechanism for working with a Tester.

Tester Evaluation

12.1.4 The Tester will work with the Monitoring Licensee to undertake an evaluation of the proposed Monitoring System to ensure it meets the requirements set out in the Victorian Technical Standards.

12.1.5 The Tester will provide a report to the Commission based on the following:

i) The system integrity and reliability;

ii) Whether the system meets all the legislative, technical, and reporting requirements;

iii) Whether the controls and procedures required exist and are effective; and

iv) System baseline and Network Security Policy Document for future approval.

Facilities for a Tester

12.1.6 The Licensee must make the appropriate facilities available to a Tester in the course of the Licensee's engagement of a Tester in order that a Tester is in a position to conduct an adequate evaluation of the system (or changes to an approved the system) and make its recommendation to the Commission accordingly.

Test Environment

12.1.7 The Licensee must ensure that upgrades to the CMCS and associated Monitoring Equipment can be adequately tested in an appropriate test environment using a test system that is functionally, but not necessarily physically, identical to that proposed for use in production.

12.1.8 The test system is not to share any hardware with the production system, except for a power source and other items of hardware for which express permission for exclusion must be sought from the Commission.

12.1.9 There must be a method to verify that the baseline software evaluated and recommended for approval (by a Tester) on the test system is the same baseline software that has been migrated to the production system following the baseline software's approval.

12.1.10 The test system must be able to interface to Venues in a wide range of geographical areas.

Failure Modes and Recovery Testing

12.1.11 The Licensee must ensure that a Tester is able to test the Host CMCS for resilience, recoverability and continuity of service, including but not limited to conditions for:

i) Failure of Host CMCS power supply;

ii) Total power failure of the Host CMCS site:

a) For a short period (e.g. 30 seconds); or

b) For a long period (e.g. 30 minutes);

iii) Verifying there is no single point of failure;

iv) Individual server capability to sustain persistent load;

v) Guaranteed messaging;

vi) Failure of critical components, including but not limited to processors, handlers, gateways, API's[24], and communication protocols or similar;

vii) Failure of critical storage devices, including those holding data files and databases critical to the operation;

viii) Failure of Host CMCS I/O channels;

ix) Failure of links with remote interface points; and

x) Host CMCS operator error, including but not limited to invalid Data entry.

12.2 System Testing Requirements

Testing Requirements and Tester Recommendation

12.2.1 The security and controls, functional specifications, and all the requirements of the system are to be evaluated and recommended by a Tester listed on the Roll of Manufacturers, Suppliers and Testers as defined in the Act.

12.2.2 A Tester recommendation is required on:

i) The system integrity and reliability;

ii) Whether the system meets all the legislative, technical, and reporting requirements;

iii) Whether the controls and procedures required exist and are effective; and

iv) The System Baseline Document and Network Security Policy Document for future approval.

[24] Application Programming Interface

Associated Systems Requirements

12.2.3 All the systems associated with the CMCS are required to be tested for reliability in processing and delivering all transactions for the CMCS.

12.2.4 There must be adequate security arrangements and controls between the approved CMCS and the associated systems, and these arrangements and controls must form part of the independent assessment and Tester’s recommendation.

Environmental Testing

12.2.5 Suppliers of Monitoring Equipment are to provide information as to the range of environmental extremes at which Monitoring Equipment will continue to operate normally and must have conducted environmental testing to demonstrate the equipment’s specified maximum and minimum extremes of temperature and humidity.

12.2.6 The Commission requires the equipment to run within the equipment’s own environmental specifications.

13 Document Information

13.1 Document details

Criteria	Details
Document title:	Victorian Central Monitoring and Control System Requirements Document
Document owner:	Director, Gambling Licences Project, Commission
Document author:	Gambling Licences Project, Commission

13.2 Version control

Version	Date	Description	Author
V1.0	25/06/09	First public Draft CMCS Requirements Document	CCommission
V2.0	18/09/09	Revised Draft CMCS Requirements Document	Commission
V3.0	03/12/09	Revised Draft CMCS Requirements Document	Commission
V4.0	15/04/10	Revised Draft CMCS Requirements Document (ancillary gaming requirements section 11 of V3.0 removed)	Commission
V5.0	06/04/11	Revised Draft CMCS Requirements Document (approved Monitoring Equipment, section 3.4)	Commission

13.3 Reference material

Acronyms	Description
CMCS	Central Monitoring and Control System
GLP	Gambling Licences Project
VCR	Victorian CMCS Requirements document
VSD	Victorian Systems Document, predecessor to the VCR document

13.4 Approvals

Name	Position	Function
Commission	The Commission	Approve

14
Related Documents

Document Title	Version
Australian/New Zealand Gaming Machine National Standard	V10.0
Victorian Appendix to the Australian/New Zealand Gaming Machine National Standard	V10.0
Victorian Systems Document	V2.0
Commission Standards	Refer Glossary

15

Appendix A - Venue Operator Requirements

This Appendix sets out the requirements for Venue Operators in relation to the CMCS implemented by the Licensee.

15.1 General

15.1.1 It is the Venue Operators responsibilities to have installed and maintained all Gaming Equipment and Venue Signage. Any third party gaming systems are also ultimately the responsibility of the Venue Operator.

15.1.2 It is the Venue Operator's responsibility to:

i) Fully operate and manage all aspects of the EGMs including cash handling;

ii) Operate linked jackpots within the Venue or in conjunction with other Venues with which linked jackpot arrangements[25] have been made;

iii) Provide accurate configuration and parameter information for EGMs and jackpots to the Licensee;

iv) Process and correct potential security breaches as advised by Significant Events from the Licensee and the CMCS; and

v) Provide technical assistance on request from the Commission to assist Commission Inspector's in the conduct of technical compliance.

15.2 Retention of Unclaimed Moneys

15.2.1 The Venue Operator must maintain a register of all prize money that has not been claimed after a time set in accordance with the Unclaimed Money Act 2008.

15.2.2 Retention of unclaimed moneys must be treated in accordance with the Unclaimed Money Act 2008.

[25] Linked jackpot arrangements has the same meaning as defined in the Act.

15.3 Jackpots

Fixed Prize Jackpots

15.3.1 Jackpots, which pay fixed prizes when won, must meet the Commission's maximum prize limitations. If the jackpot win pays a non-cash prize the following rules apply:

i) The Commission will deem the value of the prize for the purposes of settlement with the Jackpot Pool, to be the Venue Operator's purchase price of the prize. Documentation substantiating the actual purchase price must be maintained by the Venue Operator and made available to the Commission upon request;

ii) When requesting approval for new jackpots with non-cash prizes, the Venue Operator must submit the public's perceived "retail" value of the prize as well as the actual purchase price; and

iii) The Venue Operator must declare that any amount in (i) above is not subject to any other discount or perceived secret commission.

16
Appendix B - Jackpots

This appendix is provided as background information to current Gaming Machine Jackpots operating in Victoria.

16.1 Jackpot Types

Standalone versus Linked

16.1.1 Standalone jackpots are those that are self-contained within the EGM.

16.1.2 Linked jackpots are those that operate in two or more EGMs and are controlled by external devices known normally as a Jackpot System or Jackpot Controller.

16.1.3 It is possible to have Standalone Jackpot EGMs that are also in one or more Linked Jackpots.

Game Determined versus Mystery

16.1.4 Game determined jackpot means that the trigger for winning a jackpot is as a result of the outcome of a Game.

16.1.5 Mystery determined means that the determination of the jackpot win is not related to the Game outcome but instead by some non-Game determined event, generally by a random event.

EGM Determined versus System Determined

16.1.6 EGM determined means that the trigger for winning a jackpot is determined by the Gaming Machine itself.

16.1.7 Note that the EGM determined jackpots might be either Game determined or mystery determined.

16.1.8 System determined means that an external Jackpot System/Controller makes the determination of the jackpot win, generally by a random event.

16.2 Jackpot Prizes

16.2.1 There are two types of jackpot prizes:

i) Variable prizes – the jackpot increments by a proportion of each participating wager. When the jackpot is won, the current value of that jackpot is paid to the winner; and

ii) Fixed prizes – the winner is paid a fixed amount that was advertised in advance of the start of the jackpot Game. There can be two kinds of these:

a) Cash fixed prize; and

b) Merchandise.

16.3 Jackpot Levels

16.3.1 A typical jackpot arrangement will have an EGM in multiple jackpots, also known as jackpot levels.

16.3.2 A typical Game determined jackpot EGM would have three or four levels with the levels having increasingly less probable chance of the outcomes.

16.4 Jackpot Displays

16.4.1 Jackpot Displays provide information to players that the Commission consider must be available, such as current jackpot amounts and jackpot winners.

16.4.2 Jackpot Displays are mandated for all variable type jackpots and, if there is no form of display available to the players, the jackpot must be shut down.

16.4.3 There are two types of jackpot displays:

i) In built displays in the individual EGM; and

ii) Overhead displays which tend to sit above banks or groups of EGMs.

16.5 Jackpot Parameters

16.5.1 The following sections describe the most important parameters relating to jackpots.

Game Determined Jackpots

16.5.2 In Game determined jackpots, there are two main system parameters for each jackpot level:

i) The start-up value or amount for the jackpot when first run or just after it has been won; and

ii) The Increment percentage which is the proportion of each wager that is put into the jackpot as it occurs.

16.5.3 An additional parameter, the probability of winning the jackpot, is applicable to all participating EGMs.

Mystery Jackpots

16.5.4 In most implementations, there are three parameters that drive each level of mystery jackpot:

i) The start-up value or amount for the jackpot when first run or just after it has been won.

ii) The maximum Jackpot amount; and

iii) The Increment percentage which is the amount of each wager that is put into the jackpot as it occurs.

16.5.5 Note that in EGM determined mystery jackpots, there may not be a maximum parameter but instead this may be replaced by a probability of the mystery win occurring.

Participating EGMs

16.5.6 For any jackpot a list of participating EGMs must be maintained.

16.5.7 The probability of winning each level of the jackpot must be the same for each EGM in the participation list.

16.6 Taxation Basis

16.6.1 The Act enables gaming operators to deduct “jackpot contributions” from their revenue before determining taxation.

16.6.2 Furthermore, the Act enables the jackpot contributions to be deducted when they are made rather than when they are paid out.

16.6.3 Operators have two choices for claiming deductions:

i) Deduct jackpot payouts when they occur; or

ii) “Virtualise” the player return for each jackpot level to calculate a percentage with the probabilistic return and deduct that percentage from revenue as Games are played.

16.7 Jackpot Pools

16.7.1 For each jackpot level, there is a current “pool” which represents the start-up value and the increments contributed since the last time that pool had been won.

17
Appendix C - Scheduled Tasks

This appendix details the schedule of tasks expected to be carried out by the Licensee when operating a CMCS in Victoria.

17.1 Daily Tasks

17.1.1 The following table summarises the tasks, based on the detail contained in related document references, that the Commission expects the Licensee to carry out on a daily basis.

Task	Description	Document Reference
Database Backups	There must be periodic back-ups (at least daily) of the variable database files on the CMCS's storage devices.	4.9.14
Financial Gaming Activity Reports	Reports to verify financial gaming activity on all Gaming Machines (and jackpots) connected to the CMCS on a daily basis.	4.12.12 i)
Link to Commission Computing Facilities	This link is for the purpose of down loading financial, Game Play statistical Data Significant Events and jackpot Data on a daily basis (or at a frequency agreed by the Commission). Such Data must be extracted from the main CMCS database to a special Commission database.	4.12.25
Disable Gaming Equipment	The CMCS must disable Gaming Equipment, for Game Play, at the end of the current day's liquor license hours for that site.	7.2.96 i)
Accounting Reconciliation	Accounting reconciliations are to be performed at least daily by the Licensee at the Venue level for Venue level jackpots, and at wide area level for wide area	8.3.5

Task	Description	Document Reference
	jackpots. These reconciliations must be provided to the Venue Operator as required.	
Automatic Verification of Configuration	The configuration of host monitoring systems and network management systems must not be changed without approval from the Commission. Automatic verification of the configuration of these systems must be performed at least daily.	9.3.29
Verify Executable Software	There must be a method available to verify that the executable software that has been used during the testing process is identical to that which is to operate on the live system. This verification procedure must occur when new software is installed, at the start of each trading day by the Licensee and randomly on demand by the Commission.	7.2.11 vi)
Type 4 Events Report	The CMCS must provide a daily Type 4 events report.	10.1.3
Gaming Machine Off Line Report	Every day the CMCS must generate an electronic media report of all Gaming Machines reported as being off-line and with zero financial transactions for the previous day as a Gaming Machine may be on-line all day but experience no transactions.	10.2.6
Summary Data	Summary Data on Games played, bets placed and prizes (including jackpots) won for each Gaming Machine {Type 1}: it is mandatory that this Data is gathered at least daily.	4.12.16
Mandatory Meters	This meter information must be forwarded to the CMCS at a period no less frequent than the Daily reconciliation (Poll) process.	4.12.16
Unclaimed Cash Tickets	The CMCS must provide information for daily reconciliation of redeemed and unclaimed cash tickets, which must be conducted daily by the Licensee, and also the Venue Operator.	4.7

17.2 Weekly Tasks

17.2.1 The following table summarises the tasks, based on the detail contained in related document references, that the Commission expects the Licensee to carry out on a weekly basis.

Task	Description	Document Reference
Financial Gaming Activity Reports	Reports to verify financial gaming activity on all Gaming Machines (and jackpots) connected to the CMCS on a weekly basis.	4.12.12 i)

17.3 Monthly Tasks

17.3.1 The following table summarises the tasks, based on the detail contained in related document references, that the Commission expects the Licensee to carry out on a monthly basis.

Task	Description	Document Reference
Financial Gaming Activity Reports	Reports to verify financial gaming activity on all Gaming Machines (and jackpots) connected to the CMCS on a monthly basis.	4.12.12 i)
Tax Advice	Calculate and advise the Commission and each Venue Operator of the respective tax to be paid by the Venue Operator each month.	4.12.12 i)

17.4 Three-Monthly Tasks

17.4.1 The following table summarises the tasks, based on the detail contained in related document references, that the Commission expects the Licensee to carry out every three months.

Task	Description	Document Reference

Task	Description	Document Reference
Power Supply	The UPS, stand-by generator, emergency lighting and any systems or procedures referred to herein, or otherwise essential to the operation of a CMCS, must be tested at least every three months.	4.2.7
Security Reviews	Adequate system security procedures and policies are in place, including security reviews conducted at least every three months.	4.8.12 i)

17.5 Six-Monthly Tasks

17.5.1 The following table summarises the tasks, based on the detail contained in related document references, that the Commission expects the Licensee to carry out every six months.

Task	Description	Document Reference
System and Network Penetration Test	The Licensee must ensure that an accredited external and independent Information Technology Network and Security Testing company undertakes system and network penetration testing on its CMCS and CMCS related Monitoring Equipment every six months and provide a written report of its findings.	4.8.11

17.6 Periodic Tasks

17.6.1 The following table summarises the tasks, based on the detail contained in related document references, that the Commission expects the Licensee to carry out in accordance with a period or frequency that is approved by the Commission.

Task	Description	Document Reference
Financial	Commission approval must be obtained for	4.12.9

Task	Description	Document Reference
Verification Data Collection	the frequency of financial verification Data collection.	
Accumulated Jackpot Increments	If each individual bet is not to be passed to the CMCS, the local computers or controllers must accumulate jackpot increments and forward them frequently and accurately to the central host. Commission approval must be obtained for this period.	8.1.11
Jackpot Meter Information	The Jackpot Meter Information must be periodically transferred from the Jackpot Controller to the CMCS and recorded there. Commission approval must be obtained for this period.	8.1.48

End of Document