VICTORIAN PRE-COMMITMENT SYSTEM REQUIREMENTS DOCUMENT

February 2015

Version 1.0

Victorian Commission for Gambling and Liquor Regulation

State Government Victoria

Table of Contents

1 GLOSSARY 7

2 FOREWORD 14

2.1 Pre-commitment framework 14

3 INTRODUCTION 15

3.1 General information 15

The Act 15

Objectives 16

Document scope 16

General principles 16

ICT service management framework 17

3.2 Operational requirements 17

Provision of information 17

System performance standards 17

Responsibilities 18

3.3 Approved PCS equipment 18

Approval of PCS equipment 18

3.4 Victorian Technical Standards 18

3.5 External references 19

4 PRE-COMMITMENT MONITORING AND CONTROL 20

4.1 PCS environment 20

4.2 Host PCS system accommodation 22

Physical security 22

Help desk system 23

4.3 PCS system 23

PCS integration and interface to CMCS and EGMs 24

Handshake and signature checking 24

System baseline document 25

Emergency changes 26

PCS service delivery procedures 27

PCS software quality 27

4.4 Central logging of information 27

4.5 Significant events 28

Storage of significant events 28

Recovery of significant events 28

Creation of significant events 29

4.6 PCS security 29

System audit 30

4.7 PCS recovery 31

Host PCS recovery 31

Transaction logging 31

Format of records 32

Disaster recovery and business continuity 32
System data recovery 33
Central site failure modes and recovery 33
4.8 Data security 34
Encryption of stored data 34
PIN and password management 34
4.9 PCS integrity 34
Security of event and transaction logs 34
Multiple log files 35
Data and event collection 35
Documentation and reporting 35
Required reports 35
PCS interfaces to sub-systems 36
Link to Commission computing facilities 36
Inspection 37

5 VENUE REQUIREMENTS 38

5.1 General 38
5.2 Responsibilities 38
Hardware and infrastructure 38
Operations 38
Venue operators 38
5.3 Maintenance........ 38
Retention of data 39
Maintenance not to infringe approval 39
5.4 Venue keys and locks 39
Key control 39
5.5 Movement, upgrade, modification of PCS equipment 40
5.6 Destruction of PCS equipment 40
5.7 Venue environment 40

6 PRE-COMMITMENT EQUIPMENT (HARDWARE) 41

6.1 Hardware requirements........ 41
Information display 41
Card reading device 41
Device I/O 41
6.2 Maintenance requirements........ 41
Retention of data 41
Maintenance not to infringe approval 42

7 PRE-COMMITMENT EQUIPMENT (SOFTWARE) 43

7.1 Software requirements 43
7.2 Software quality requirements........ 43
Source code 43
Source compilation 43
Source control and upgrade 44
Software functions provided 44

Software verification during development 45

8 PLAYER ACCOUNT REQUIREMENTS 46

8.1 Player accounts 46

8.2 Creation of player accounts 46

Registered player account 46

Casual player account 46

Non player accounts 46

8.3 Privacy of registered player information 47

8.4 Player accounts maintenance 47

8.5 Player statements 48

8.6 Cancelled player accounts 48

8.7 Player activity data 48

9 PRE-COMMITMENT SERVICES 49

9.1 Common functional requirements 49

9.2 Access to pre-commitment 49

Player access 49

Venue operator access 50

Help desk access 50

Inspectors 50

9.3 Player registration and cancellation 50

Registration 51

Pre-commitment card 51

Cancellation 51

9.4 Pre-commitment limits 52

9.5 Tracking Play 53

9.6 Reporting 55

9.7 System performance 55

10 INTEGRATION WITH LOYALTY SYSTEMS 56

10.1 Infrastructure and data 56

10.2 Functional requirements 57

Dual player cards 57

Messaging 57

Loyalty points accumulation 57

11 NETWORK AND COMMUNICATIONS 58

11.1 Communications requirements 58

Communication scheme 58

Data communications 58

11.2 Cryptographic data security 59

Introduction 59

Requirement for cryptographic data security 60

Encryption algorithm approval 60

Message authentication algorithm approval 61

Encryption keys 61
11.3 Network requirements 61
General 61
Network baseline 61
Physical requirements 61
Network documentation 62
Connection of devices to networks inside a baseline envelope 62
Communications within a baseline envelope 62
Communications between separate baseline envelopes 62
Communications to devices outside a baseline envelope (firewall) 63
Host monitoring systems and network management systems 64
Internet connections 65
Verification tools 65
11.4 Wireless communication 65

12 PRE-COMMITMENT SIGNIFICANT EVENTS 66

12.1 General 66
12.2 Significant events 66

13 SUBMISSION REQUIREMENTS 68

13.1 General 68
Environmental testing 68
13.2 PCS/Site operator requirements 68
13.3 Player information 69
13.4 Communications 69
Authentication and encryption 69
PCS internal network architecture 69
Third party connections 71
PCS host computers 71
PCS software 73
PCS operations 73

14 TESTING REQUIREMENTS 74

14.1 Inspection and testing 74
Tester evaluation 75
Facilities for a tester 75
Test environment 75
Failure modes and recovery testing 76
14.2 System testing requirements 76
Testing requirements and tester recommendation 76
Associated systems requirements 76

15 DOCUMENT INFORMATION 77

15.1 Document details 77
15.2 Version control 77
15.3 Approvals 77

16 RELATED DOCUMENTS 78

17 APPENDIX A - VENUE OPERATOR REQUIREMENTS 79

17.1 General... 79

1 Glossary

This chapter sets out the glossary of standard terms and abbreviations used by the Commission and relevant to the Pre-commitment System Requirements document.

Term or Abbreviation	Description
Act	Means the *Gambling Regulation Act 2003*, as amended from time to time. Viewed 25 February 2015
Ancillary Services Systems	A system, including software and hardware that caters for provision of additional services offered to a venue provider that may connect to gaming and/or monitoring and/or PCS equipment.
API	Application Programming Interface.
Baseline	A snapshot of an evolving system. The baseline also defines an envelope around a system (defined by the service provider 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).
Card encoder	Means a device that is capable of recording information onto a player card as defined in section 3.8A.1 of the Act.
Card reader	Means a device that is capable of reading information stored on a player card as defined in section 3.8A.1 of the Act.
Casual player	Means a player who has been issued with a casual player Card, as defined in the Regulations.
Central Site	The location of the PCS host.
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.
Commission	The Victorian Commission for Gambling and Liquor Regulation established under the *Victorian Commission for Liquor and Gambling Regulation Act 2011* or any successor body. Viewed on 25 February 2015.
Commission Standards	The relevant Commission gaming standards are the standards referred to in section 3.5.3 of the Act.
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.

Term or Abbreviation	Description
Critical data	Memory locations storing information but not limited to: i). security events of Type R which have not been forwarded to the host CMCS ii). mandatory metering information iii). current game information iv). any changeable configuration information v). current credit amount vi). any PCS data associated with the cryptographic data security requirements identified at 11.2.4 and 8.7.
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 service provider to the service provider's specifications.
Data	Means all data and expressions of data contained in, or processed or generated by, the pre-commitment system including without limitation: i). All data and expressions of data comprising reports generated by the pre-commitment system ii). All data and expression of data about or relating to or generated by agents and contractors stored within the pre-commitment system.
Dual player card	Means a player card that allows a registered player to access both their pre-commitment account and an account they hold with a loyalty scheme provider.
Dynamic activity statement	Means a statement generated by the pre-commitment system, detailing a player’s use of gaming machines during a reporting period specified by the player, based on filters selected by the player.
EGM	Electronic Gaming Machine – has the same meaning as Gaming Machine.
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.
Firewall	Part of a computer system or network that is designed to block unauthorised access while permitting authorised communications.
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 play	Refer to Play.
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 Monitoring 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 pre-commitment equipment.
Help desk	A service by the service provider that provides information and assistance to public, players and PCS users.
ICT	Information Communications Technology – a generic name used to describe all technologies used by computers to communicate.
Interactive display screen	Means a device that is capable of accepting input from, and displaying information to, the player of the gaming machine on which the device is installed as defined in the Act.
Inspector(s)	A person who is appointed under Part 4 section 40 of the VCGLR Act to represent the Commission in undertaking inspections of the PCS.
Inspector card	Means a card that enables an Inspector to access the pre-commitment system.
I/O channel	The physical interface that controls the transfer of data between the computer and peripheral devices.
Jackpot system	A system to allow the operation of a Jackpot, typically made up of: • Jackpot Controller • Jackpot Display Interface • Jackpot Display • Network components.
Kiosk	Means a device, incorporating a card reader that allows a player to access information produced or stored by a pre-commitment system or loyalty scheme as defined in the Act.
LAN	Local area network is a computer network that interconnects computers and devices within a limited area.
Monitoring licence	Means the licence granted and issued under the Act by the Minister to authorise the conduct of the gaming monitoring activities.
Monitoring licensee	The holder of the Licence granted and issued under the Act by the Minister to authorise the conduct of the gaming monitoring activities.
Limit	Means a net loss limit and /or time limit.
Limit period	Means a daily, weekly or other period as allowed by the pre-commitment system over which a limit is calculated, as selected by the player.

Term or Abbreviation	Description
Limit reached message	Means a message notifying a player that a limit has been reached.
Limit threshold	Means a percentage value of a player's limit(s).
Limit threshold message	Means a message notifying a player that a limit threshold has been reached,
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.
Loyalty scheme	Has the same meaning as defined in section 1.3 of the Act
Loyalty scheme ID	A unique identifier assigned to players that have registered for a loyalty scheme. Players can be members of multiple loyalty schemes and have a different loyalty scheme identifier for each loyalty scheme they are registered with.
OLGR	Office of Liquor, Gaming and Racing within the Department of Justice & Regulation.
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. The gaming equipment's computer can only perform meter incrementing. The meter is read by human inspection of the meter display. • A storage area within some form of computer memory (for example disk or RAM) into which the computer's software is programmed to store and update the current count of the metered quantity.
Minister	The Victorian Minister responsible for the regulation of 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.
Multi-function support interface	Software/hardware interface that facilitates connection to the gaming machine devices and access to player activity data for ancillary services systems.
Network policy document	A document describing the end-to-end network topology of the PCS and is the responsibility of the service provider to prepare as part of its submission to the Commission when obtaining approval for the PCS.
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).
PAE	Refer Player account equipment
PCS equipment	Pre-commitment system equipment located at central site, or, at venues, including the communications equipment for provision of WAN and venue LAN connectivity The equipment referred to in section 3.1.7 of this document.
Peripheral equipment / devices	An external device, such as a printer, a disk drive, or a keyboard, connected to a PCS host or venue PCS component.

Term or Abbreviation	Description
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.
Player	Has the same meaning as either a registered player or a casual player.
Player account equipment (PAE)	Has the same meaning as defined in 3.8A.1 in the Act and includes player card.
Player service point	Has the same meaning as defined in the Regulations.
Pre-commitment	A mechanism to allow players to stay in control of their gambling and make informed decisions about their play.
Pre-commitment activities	Means the establishment, operation and maintenance of the pre-commitment system, the provision of Pre-commitment services and the sale, supply and possession of pre-commitment equipment in accordance with section Part 8A of the Act and the 'Scope of Services' set out in the Monitoring licence and Pre-commitment Related Agreement.
Pre-commitment equipment	Refer PCS equipment.
Pre-commitment ID	The unique sequence of numbers assigned to each player that identifies them in the pre-commitment system.
Pre-commitment related agreement	Means the Pre-commitment related agreement entered into between the Minister and the service provider under the Act.
Pre-commitment scheme	A scheme mandated by the Government of Victoria to assist players who have registered to do so track their play against pre-set time and monetary limits.
Pre-commitment session	Period of time when the pre-commitment system tracks the gaming activities of a player and commences when PCS registers a valid PIN entered after the insertion of a card and concludes of the removal of the card at the gaming machine.
Pre-commitment system (PCS)	Means the electronic pre-commitment system referred to in Part 8A of the Act and includes, without limitation, all adaptations, modifications, enhancements to that system made at any time before or during the Term.
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.
Registered player	Means a player who has: ▪ Successfully registered their request for a pre-commitment account; and ▪ Been issued with a pre-commitment ID by the pre-commitment system.
Regulations	Means the Gambling Regulation (Pre-commitment and loyalty scheme) Regulations 2014, as amended from time to time. Viewed 25 February 2015.

Term or Abbreviation	Description
Related agreements	Has the same meaning as set out in the Monitoring Licence granted and issued under the Act to the service provider.
Responsible Gambling Ministerial Advisory Council	The pre-eminent source of stakeholder advice to the Minister on responsible gambling.
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”.
Roll of Manufacturers, Suppliers and Testers (the Roll)	Has the same meaning as defined in the Act.
Service provider	The holder of the Licence granted and issued under the Act by the Minister to provide, operate and maintain a pre-commitment system.
SIA	Security integrity and authentication process. This process is to validate and verify the system baseline executable files (and selected command utilities) in order to confirm that the configuration of the system is operating in an approved state.
Significant event	Has the same meaning as defined in the Act.
Site controller	A device located at the venue and used to collect information from each gaming machine of that venue.
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.
Technician card	Means a card that enables a person listed on the Roll to access the pre-commitment system.
Tester	Means a tester listed on the Roll as described in the Chapter 3 of the Act.
Touch screen	A video monitor with a special surface screen that can interact with the user of a gaming device or PAE 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. This document refers to the 31 January 2012 version.
Venue operator	The holder of a venue operator’s licence as defined in the Act.
Venue	Has the same meaning as an approved gaming venue as defined in the Act, as well as the Melbourne casino.
Venue equipment	Equipment installed and/or operated by the venue operator for gaming and other purposes

Term or Abbreviation	Description
Venue manager card	Means a card that enables a venue manager to access the pre-commitment system.
Venue signage	Non-gaming based displays within a venue, for example 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 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.
Victorian Technical Standards	Means the current versions of the Standards for approval of technical equipment and systems relevant to section 3 of the Act and the Commission's standards. Refer to section 3.4.
VPSR	Victorian Pre-commitment System Requirements, this document
WAN	Wide area network: a computer network that covers a broad physical area.

2 Foreword

This chapter introduces the background to the Victorian Pre-commitment System Requirements document.

2.1 Pre-commitment framework

2.1.1 Gambling Regulation Amendment (Pre-commitment) Bill 2012 contains legislative amendments to the *Gambling Regulation Act 2003* (the Act) to implement the Victorian Government's pre-commitment policy.

2.1.2 Under the proposed arrangements, the Pre-commitment service provider arrangement will be offered to the licensed Monitoring Operator who will provide and operate a fit for purpose pre-commitment system to enable players to utilise the pre-commitment scheme in all Victorian gaming venues, including the Melbourne casino.

2.1.3 The objective of the Victorian Pre-commitment System (PCS) is to facilitate and support the Victorian Pre-commitment Scheme across all venues.

3 Introduction

This chapter introduces the context and the purpose of the Victorian Pre-commitment System Requirements document.

3.1 General information

3.1.1 This document must be read in conjunction with the Monitoring Licence and related agreements.

3.1.2 Requirements of the service provider set out in the VCR will take precedence relative to the requirements set out below, i.e. these requirements are supplementary to those set out in the VCR, and the service provider's system must be compliant with the requirements of the VCR prior to undertaking the establishment of a PCS.

3.1.3 This Victorian PCS Requirements document (VPSR) contains the system related requirements for the pre-commitment system.

3.1.4 This document will be used by the service provider and tester(s) to evaluate the system for compliance with the PCS requirements, or to evaluate changes to a previously approved system for approval.

3.1.5 This document will be used by the Commission to evaluate compliance by a service provider with the Monitoring Licence and Pre-commitment related agreement, and to evaluate changes to a previously approved PCS, in accordance with the Act.

3.1.6 All references in this document pertaining to the service provider refer to the entity appointed to conduct the pre-commitment activity identified by its Agreement.

3.1.7 The PCS consists of any instrument, device or computer hardware or software or any other equipment that the service provider proposes to use, or will cause or permit to be used, for the conduct of the pre-commitment activities permitted by the Act and, the Pre-commitment related agreement.

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 Monitoring Licence and any related agreement's conditions.

3.1.10 In approving the PCS 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 Pre-commitment Scheme.

Objectives

3.1.11 The Commission sets high systems integrity standards for gaming equipment, monitoring equipment and pre-commitment equipment operating in Victoria for the purpose of ensuring that:

i). the system operates in accordance with the Monitoring License and the related agreement)

ii). the system operates in accordance the set by the Pre-commitment related agreement

iii). the system operates in a manner that is auditable, reliable and secure.

3.1.12 Matters arising from the testing of pre-commitment equipment that have 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 service provider, 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 service provider according to the Monitoring Licence and Pre-commitment related agreement at central locations and venues in Victoria and at a disaster recovery site in Australia.

General principles

3.1.14 The PCS must fully implement the pre-commitment requirements and pre-commitment services as specified in the Pre-commitment related agreement.

3.1.15 Documentation received by the Commission and user-facing messages must be in English and be both grammatically and syntactically correct.

ICT service management framework

3.1.16 In order to ensure that the PCS and associated equipment operate as approved by the Commission, the service provider must establish and maintain policies, standards and procedures that the service provider will use to develop, implement and operate the PCS, 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). service continuity management

xii). security management

xiii). ICT infrastructure management.

3.2 Operational requirements

Provision of information

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

3.2.2 When evaluating the PCS for approval, the service provider must provide sufficient information and documentation to enable a full determination of the PCS level of compliance with this system requirements document.

System performance standards

3.2.3 The PCS must be capable of meeting the performance standards set out in the Pre-commitment related agreement and the requirements set in section 9.7 of this document.

3.2.4 Communication systems forming part of or used in association or connection with the PCS must be capable of meeting the performance standards set out in the Pre-commitment related agreement.

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

3.2.6 The PCS must be capable, at all times, of determining whether all agreed upon PCS components and peripheral equipment connected to it, are functioning and whether the agreed player account equipment (PAE) components are connected.

Responsibilities

3.2.7 The service provider must adhere to the responsibilities detailed in the Act, the Monitoring Licence and related agreements.

3.3 Approved PCS equipment

Approval of PCS equipment

3.3.1 Only approved PCS equipment may be operated in Victoria.

3.3.2 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 and pre-commitment as determined by the Commission becomes part of the PCS.

3.3.3 A component of the baseline PCS may have multiple suppliers of major assemblies, but the Commission must approve each component from each supplier. Off the shelf and custom built components of the PCS are required to meet a minimum standard equivalent to the equipment submitted for approval.

3.4 Victorian Technical Standards

3.4.1 Some requirements in this document (VPSR) are common to the Victorian Technical Standards and hence may refer to the following documents:

i). Victorian Central Monitoring and Control System Requirements (VCR) document issued by the Commission, as amended by the Commission from time to time, viewed at 25 February 2015.

ii). Australia/New Zealand Gaming Machine National Standard (National Standard), viewed at 25 February 2015.

iii). Victorian Appendix to the Australia/New Zealand Gaming Machine National Standard (Victorian Appendix), viewed at 25 February 2015.

iv). Victorian Player Account Equipment Technical Requirements document issued by the Commission, as amended by the Commission from time to time, viewed at 25 February 2015.

v). Victorian Pre-commitment System Requirements document (this document) issued by the Commission, as amended by the Commission from time to time.

vi). Related technical standards for gambling industry.

3.5 External references

i). Australian Government Information and Communications Technology Security Manual (ISM) – Controls (2014) www.asd.gov.au/infosec/ism/index.htm, viewed at 25 February 2015.

ii). Victorian Government Website Management Framework – Accessibility (v3.1)

www.digital.vic.gov.au/resources/online-and-mobile/, viewed at 25 February 2015.

4 Pre-commitment monitoring and control

This chapter sets out the pre-commitment system requirements that must be met for the service provider's operation in Victoria.

4.1 PCS environment

4.1.1 The Commission requires that the service provider implement a computerised Pre-commitment system capable of interfacing with all gaming devices at all gaming venues in accordance with the Act, the Monitoring Licence and related agreements and, additional functions as determined by the Commission from time to time.

4.1.2 The system must not result, either directly or indirectly, in an exclusive arrangement for the operation of gaming machines and venue management systems.

4.1.3 The system must not affect the integrity of the gaming machines and the monitoring system as approved by the Victorian Commission for Gambling and Liquor Regulation (VCGLR) for gaming machine play.

4.1.4 PCS must include at a minimum:

i). EGM interface board (if applicable)

ii). Site controller

iii). Telecommunications network (Local Area Network (LAN) and Wide Area Network (WAN))

iv). Network interfaces.

v). Central system (hardware and software) including:

a) PCS central database

b) PCS host

c) PCS website.

iv). PCS service and support resources

v). PCS processes and procedures.

4.1.5 The system has the following physical interfaces:

i). kiosk – *within an approved venue*

ii). card encoder – *at the player service point only*

iii). card reader – *at the kiosk, player service point and EGM*

iv). the relevant monitoring system components – *at an approved venue*

v). key pad – *at the player service point*

vi). interactive touch screen display screen – *at the kiosk and EGM*.

4.1.6 Co-utilisation of existing CMCS infrastructure and system components for the purposes of pre-commitment is permitted.

4.1.7 The PCS 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 that 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 that 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.

4.1.8 The PCS shall be designed in consideration of the 'Victorian Government Website Management Framework – Accessibility standard'[1], available from Digital Government.

[1] www.digital.vic.gov.au/wp-content/uploads/2014/07/WEB-STD-05-WMF-Accessibility-v3.1.pdf, viewed on 25 February 2015.

4.1.9 The system must be flexible and scalable in order to cater for:

i). changes in requirements and standards (as determined from time to time by the Victorian Government and VCGLR)

ii). advances in technology

iii). configurable items (as detailed in the Pre-commitment related agreement).

4.1.10 The PCS solution supplied by the service provider must have sufficient capacity (processing, memory, communications interfaces and hard disk storage) and redundancy to connect, maintain connection and efficiently provide pre-commitment Services during the term:

i). To support up to 30,000 gaming machines in venues throughout Victoria

ii). To support 30,000 concurrent players at the gaming machines

iii). To support at minimum 500,000 player records.

4.1.11 The computer system(s) at the pre-commitment system central site must operate 24 hours a day, seven days a week throughout the pre-commitment term, excluding scheduled pre-commitment downtime approved by the Commission.

4.2 Host PCS system accommodation

Physical security

4.2.1 The host PCS 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.

4.2.4 The service provider must ensure that an accredited external and independent security testing company undertakes testing of the physical security of the computer room(s) and related PCS equipment 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 service provider with respect to all issues identified in the report.

4.2.5 All host PCS equipment within or contributing to the computer room(s) environment must meet all requirements applicable to Monitoring system as set in the following sections of the VCR:

i). power supply

ii). uninterruptible power supply

iii). stand-by generator

iv). emergency lighting

v). environmental monitoring system.

Help desk system

4.2.6 A ‘help desk’ facility must be provided in accordance with the Pre-commitment related agreement to assist participating venues, players, the public and any PCS user with questions, problems, disputes and maintenance calls.

4.2.7 The help desk operators are to have secured on-line access to the host PCS to enable them to perform activities specified in the Pre-commitment related agreement.

4.2.8 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.

4.2.9 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 person making the call

iii). the issue prompting the call

iv). details of the outcome of the call.

4.2.10 The help desk must comply with the requirements specified in the Pre-commitment related agreement.

4.3 PCS system

4.3.1 Commission approval must be obtained for the software configuration (baseline) of the PCS.

4.3.2 Commission approval must be obtained for the baseline document and any variation to the baseline document as outlined in sections 4.3.13 to 4.3.22.

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

PCS integration and interface to CMCS and EGMs

4.3.4 The PCS and PAE operation and its individual devices must not affect the EGM and/or CMCS functionality, availability security and performance.

4.3.5 PCS and PAE components and their operation must not affect any EGM or CMCS configuration, including CMCS network devices.

4.3.6 PCS must prevent data corruption in particular where database instances, tables or data are shared between the PCS and the CMCS.

4.3.7 PCS must not affect any of the CMCS or an EGM's availability and functionality in the following circumstances:

i). PCS maintenance is performed or/and components have been replaced or their software upgraded

ii). hardware or software failure of either PCS or its components

iii). PCS or it individual components are powered down or restarted

iv). PCS or its components are disconnected or stop responding

v). PCS periodic data backup

vi). PCS database failure

vii). PCS database recovery from last back-up

viii). PCS system recovery from failure at central site or at the venue.

Handshake and signature checking

4.3.8 The PCS is required to ensure the presence and connectivity of all PCS components, including the EGM pre-commitment equipment within a venue.

4.3.9 Where venue equipment includes PCS approved software, a signature check process is required on power up of the devices and upon re-establishing communication with the next device in the system hierarchy, to confirm only approved software is deployed.

4.3.10 Software signatures are to be validated by ‘higher level’ or upstream devices on the PCS network.

4.3.11 Where a handshake or signature checking process fails to meet operational criteria:

i). a record of the event is to be logged as a significant event for monitoring and analysis purposes

ii). downstream components or PAE will be denied access to associated EGM meters.

4.3.12 The service provider is to alert the respective venue operator to any devices failing the handshake and signature criteria.

System baseline document

4.3.13 The service provider must prepare and maintain a system baseline document for approval by the Commission.

4.3.14 The system baseline must include:

i). system hardware components

ii). system application/software components

iii). network and communication infrastructure components.

4.3.15 The baseline document must include – in addition to the baseline information – a network diagram and application description for all non-baseline systems, components and applications that:

i). communicate with the baseline envelope components

ii). share hardware or database instance with baseline components.

4.3.16 The service provider – with the consultation of the Commission and assistance of the tester (if necessary) – must submit to the Commission as part of system approval, the following:

i). documentation on all system components

ii). documentation on all system component related configuration items

iii). identification of those components in (i) and (ii) that are core to operating a Pre-commitment Scheme ('the system baseline').

4.3.17 The system baseline and the system baseline document must include all the core components of the PCS, including, where applicable:

i). the software used to validate and verify that the system is operating in an approved configuration

ii). application files including database stored macros and/or scripts and procedures

iii). hardware platforms

iv). operating systems

v). interface devices / modules and related software that interact with databases used by the system application

vi). interface devices and related software that interacts with any neighboring application, external system, remote outlet or third party services

vii). systems communication devices that interface with any neighboring application, external system, remote outlet or third party services or equipment

viii). all system network connection and configuration interfaces must be identified and represented in the network policy document. (refer to section 11.3) ix). identification of any operations or procedures relevant to securing and controlling of the system

x). identification of any other special operational or procedural issue that is relevant to the Commission.

4.3.18 The service provider must obtain the approval of the Commission for changes to any components identified within the baseline.

4.3.19 Each application for a change to the baseline must include a revised baseline document for verification and endorsement by the Commission.

4.3.20 Each application for a change to the baseline must be accompanied by a tester's recommendation.

4.3.21 The baseline document must specify the location of application files and configuration files.

4.3.22 The PCS must have a security integrity and authentication process (SIA) to inform, validate and verify the baseline system executable files (and selected command utilities) in order to confirm that the configuration of the system is operating in an approved state.

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

Emergency changes

4.3.24 Emergency changes to the PCS must be notified to the Commission prior to being applied. Note: this notification does not constitute approval of the change(s).

4.3.25 The notification must include a submission of the details of the problem that is causing the emergency that the changes are solely for the purpose of resolving this problem and the baseline changes required for the emergency change.

4.3.26 Before any emergency change, the service provider must instigate a PCS baseline SIA process: this is to confirm PCS is operating an approved baseline prior to the change.

4.3.27 On implementation of the Emergency change, the service provider must instigate a PCS baseline SIA process: this is to confirm PCS is operating on the emergency change baseline.

4.3.28 The service provider must have appropriate internal procedures in place to provide for internal authorisation for the change, which is to include documenting or logging the actual change or in each respect amended executable and must include appropriate levels of management sign-off.

4.3.29 A subsequent tester recommendation and an application for the Commission's final approval are required for all emergency changes. This may be submitted with the next variation to the approved baseline.

PCS service delivery procedures

4.3.30 The service provider must establish and maintain policies, procedures and standards in accordance with the operational requirements referenced in section 3.2.

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

4.3.32 Only approved application files, within the baseline, may reside on storage devices or in the memory of identified PCS components.

PCS software quality

4.3.33 Refer to section 7.2.

4.4 Central logging of information

4.4.1 Player activity data and player account data must be held for each individual player in a (backed-up) central computer system. They may also be held in intermediate points in the PCS or network.

4.4.2 The pre-commitment ID must identify the player activity and player account data.

4.4.3 The Pre-commitment system has to maintain an audit log of player account and player activity records that are created, accessed or modified.

4.4.4 At minimum, the audit logs for player account contain records with the following fields:

i). when the event occurred: date and time stamp of the event

ii). what type of event occurred: create, access, modify or significant event

iii). location of the event: such as venue identifier, device, source address

iv). if the outcome of the event is a failure

v). the user associated with initiating the event (if relevant)

vi). the player’s identifier of the player’s account.

4.4.5 At minimum, the audit logs for player activity contain records with the following fields:

i). when the event occurred: date timestamp of the event

ii). what type of event occurred: modify or significant event

iii). location of the event: such as venue identifier or device of the player’s activity record.

4.4.6 All player activity, player account, associated audit log, and PCS significant events data must be held and be able to be accessed or retrieved (either online or from back-up):

i). player activity and player account data: for 10 years

ii). PCS significant events: for two years – inline with VCR central logging. For further details on significant events, refer to sections 4.5 and 12

iii). audit log: two years.

4.4.7 All player activity, player account, associated audit log, and PCS significant events data must be available on request to assist VCGLR with audits and investigations.

4.5 Significant events

4.5.1 The service provider must establish and maintain policies, procedures and standards for reporting significant events to the Commission.

4.5.2 The significant events are described in section 12.

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 PCS or intermediate points of the PCS at the service provider’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 PCS (for example interface boards, local controllers, remote controller)

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 PCS:

i). within 10 seconds of the recording of the significant event
or
ii). as soon as connection is restored.

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 documents in section 3.4 or this document states that the PCS 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 not prescribed. However, if the standards state that PCS equipment must detect and record an event, then the pre-commitment equipment must be programmed to create internally the event and pass it to the PCS as soon as practical.

4.6 PCS security

4.6.1 The service provider must establish and maintain policies, procedures, standards and mechanisms for adequate security over the approved system to ensure continued system integrity, availability, and audit ability.

4.6.2 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.

4.6.3 The service provider 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 password policy must be enforced that is agreed between the service provider and the Commission

iii). procedures for adequate protection of passwords.

4.6.4 The service provider 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.

4.6.5 The service provider 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.

4.6.6 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.

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

4.6.8 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.

4.6.9 The service provider must ensure that access to specific functions, within the PCS 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

iii). other functions as determined by the Commission.

4.6.10 The service provider must develop and maintain policies and operating procedures to prevent unauthorised access or changes to the PCS and PCS equipment.

4.6.11 The service provider must be in accordance with AS/NZ ISO/IEC 27002:2006 and ISO/IEC 27000-Security Management System standards.

4.6.12 The service provider 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 PCS every 12 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 service provider with respect to all issues identified in the report.

System audit

4.6.13 The service provider 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 neighboring 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

xiii). emergency change control.

4.6.14 The service provider 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.

4.7 PCS recovery

Host PCS recovery

4.7.1 The service provider must have policies, procedures and standards in place in accordance with Commission guidelines for hosting PCS data and software recovery and any relevant components

Transaction logging

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

4.7.3 For transaction logging it is required that:

i). The host PCS must record in a log file or databases (including time stamp and date stamp) all vital transactions received from PCS equipment and other elements of the PCS. For the purposes of this section ‘vital transactions’ means the transactions listed in section 4.7.17.

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.

v). All adjustments or modifications to the transactions and accounts must be recorded with the host PCS operator’s user ID (and time/date-stamp).

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

4.7.5 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 records

4.7.6 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 PCS for which the transaction/event occurred

iv). any relevant data that is associated with the event

v). a unique event identifier that defines the transaction/event.

4.7.7 A list and description of all transaction/event identifiers must be provided to the Commission, and must be kept up to date by the service provider as modifications are made to the system.

Disaster recovery and business continuity

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

4.7.9 The service provider must establish and maintain policies, procedures and standards for business continuity and disaster recovery.

4.7.10 The service provider must establish and maintain a business continuity plan, and a disaster recovery plan.

4.7.11 The service provider must establish and maintain a disaster recovery test plan, including a schedule for testing – that has to be approved by the Commission – and conduct disaster recovery testing in accordance with the approved plan.

4.7.12 In the event of a disaster, there must be a method of ensuring that all data, transactions and information related to PCS be rebuilt up to the point of the disaster, or, the previous backup or restore point.

4.7.13 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.

4.7.14 There must be periodic back-ups (at least daily) of the variable database files on the host PCS storage devices.

4.7.15 The disaster recovery site must be located in Australia.

4.7.16 The disaster recovery site must meet the standards required for the primary site as set out in this document.

System data recovery

4.7.17 In the event of a failure whereby the host PCS 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). manual database updates

iii). player account and activity data

iv). audit logs

v). current system encryption keys.

4.7.18 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.

4.7.19 The solution must support standard and emergency data recovery requests.

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

Central site failure modes and recovery

4.7.21 Following any failure, it must be possible to restore the state of the host PCS and its database(s) without losing data as defined in section 4.7.1.

4.7.22 All backup or stand-by systems and associated processes, at a minimum, must be tested at least annually.

4.7.23 Some typical tests that may be implemented by the Commission or its representatives to test compliance with this and other sections of the VPSR 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, (for example 30 seconds)

vii). total power failure of the central site for a long period, (for example 30 minutes)

viii). operator error (invalid data entry, etc.).

4.8 Data security

Encryption of stored data

4.8.1 The service provider must encrypt stored system related 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) – Controls'.

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

i). PINs

ii). passwords.

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

i). encryption / decryption keys.

PIN and password management

4.8.4 If a PCS 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 meet the requirements (4.8.2) and be evaluated by the Commission prior to approval.

4.8.5 The storage of PINs and passwords is to be in an encrypted, non-reversible form. This means that if a person (authorised or not) reads the device 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.

4.9 PCS integrity

4.9.1 The service provider must establish and maintain policies, procedures and standards for configuration management, including a configuration management plan that identifies the configurable items under management.

4.9.2 Commission approval must be obtained for the hardware configuration of the PCS.

4.9.3 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

4.9.4 The system must prevent the changing of the significant events log. 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 (that is no random update methods are to be permitted).

Multiple log files

4.9.5 There must be at least two physical copies for each file and/or database that contains the vital information documented in sections 4.6 and 4.7 using secure storage methodology.

4.9.6 The service provider’s security policies, procedures and standards, and the mechanisms for ensuring system security, apply equally to production data files and databases as well as those at disaster recovery site(s) stored at rest.

Data and event collection

4.9.7 All required data as per this document must be passed to the host PCS by an approved electronic data communications means in a timely manner by schedule and/or on demand.

4.9.8 Guaranteeing the authenticity of this information at the host PCS will be one of the important aspects of the Commission's system verification and approval process.

Documentation and reporting

4.9.9 The Commission has provided details of the Commission’s reporting requirements to the service provider.

Required reports

4.9.10 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.

4.9.11 Reports that are to be supplied to the Commission must be able to be clearly printed, and be available to be:

i). exported to common electronic format(s) agreed to by the Commission

ii). printed

or

iii). both.

PCS interfaces to sub-systems

4.9.12 The Commission may approve the integration of all sub-systems or utilities with the PCS and PCS equipment in general, including but not limited to:

i). performance monitoring systems

ii). security systems

iii). network communication and monitoring

iv). application management systems

v). environmental monitoring systems

vi). any other application that is assisting in the efficient operation of a pre-commitment scheme.

4.9.13 The integration of the PCS with sub-systems or utilities must be described in the Configuration Management Plan.

Link to Commission computing facilities

4.9.14 The service provider, at the direction of the Commission or an Inspector appointed under section 10.5 of the *Gambling Regulation Act 2003*, must provide online, data-link access for the Commission to the service provider’s computer system.

4.9.15 The PCS software supplied to the Commission must provide tools and mechanisms to:

i). examine, download or print significant events

ii). request, generate, review, save and print reports.

4.9.16 The data link between the Commission and the service provider’s host PCS must implement cryptographic data security as detailed in section 11.2.

4.9.17 The data link between the Commission and the service provider’s host PCS must have a minimum data transfer rate that is sufficient for the purpose to cater for section 4.9.15.

4.9.18 For the purpose of downloading significant events, data transfers to the Commission will occur on a daily basis (or at a frequency agreed by the Commission). Such information must be extracted from the host PCS database to a special Commission database.

4.9.19 The service provider 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 PCS from Commission premises for online interrogation of such system information as significant events and reports. Such access must be read-only: that is the Commission’s representative should have no capability to alter any information on the system.

Inspection

Facilities for Inspectors

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

i). ability to determine operational hardware and software revision levels

ii). ability to verify that PCS equipment is on-line

iii). ability to verify that player account equipment at the gaming machine and on the venue floor is available and connected

iv). facilities to support an Inspector working together with an Inspector in the field

v). other facilities to assist the conduct of Inspectors' tasks as necessary for a particular gaming system

vi). ability to review significant events and reports

vii). ability to audit logs

viii). ability to conduct a SIA

ix). provision for technical assistance to perform all the above

x). facilities (iv) and (v) to include provision and maintenance of hardware and electronic links at and to the Commission's premises

xi). provision of technical assistance on request from the Commission to assist VCGLR inspectors in the conduct of technical compliance.

5 Venue requirements

This chapter sets out the equipment requirements for operations carried out within gaming venues in Victoria.

5.1 General

5.1.1 Installation of PCS equipment must conform to the requirements set down in section 3.5.5 of the Act.

5.1.2 PCS equipment and player account equipment (PAE), is to be compliant with the requirements laid down in this document and the 'Player Account Equipment Technical Requirements'.

5.2 Responsibilities

Hardware and infrastructure

5.2.1 It is the service provider's responsibility to install and maintain all venue PCS equipment. This will include, at least:

i). PCS enabled site controller(s)

ii). interface devices exposed at the EGM for player account equipment

iii). local area network for connecting the PCS to gaming equipment within a venue

iv). wide area network for connecting the PCS to the host PCS

v). the locked cabinet that will house the pre-commitment site controller.

Operations

5.2.2 It is the service provider's responsibility to:

i). operate the PCS and manage its interfaces to the player account equipment

ii). supply the venue operators with relevant manuals and instructions for using service provider provided equipment within the venue.

Venue operators

5.2.3 Please refer to section 17.

5.3 Maintenance

5.3.1 Maintenance of PCS equipment 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 service provider.

Retention of data

5.3.2 All data stored in the PCS shall be retained during hardware maintenance and shall be protected against damage, destruction or alteration during maintenance operations (including battery replacement).

Maintenance not to infringe approval

5.3.3 Maintenance must be carried out in such a way that the 'Type Approval[2]' for any equipment is preserved.

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

5.3.5 Hardware maintenance of PCS equipment shall not be by any of the following means:

i). testing and fault diagnosis requiring the cutting of circuit board[3] 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

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.

5.3.6 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

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 PCS 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 service provider must ensure that records are kept of all locks and keys supplied and these records must be available to the Commission upon request.

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

[3] A board whose electronic components and their interconnecting circuits are mounted or etched.

5.5 Movement, upgrade, modification of PCS equipment

5.5.1 Hardware and software revision levels of each PCS equipment unit in the field must be tracked. As a minimum, records must be maintained for each device showing current revision levels of the PCS equipment, together with the corresponding unique PCS equipment identification information and current location and operational status of the PCS equipment.

5.6 Destruction of PCS equipment

5.6.1 The service provider must establish and maintain policies, standards and procedures, in accordance with the Act, relating to the destruction of PCS equipment.

5.7 Venue environment

5.7.1 The service provider 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:

iii). acceptable temperature and humidity range

iv). power supply quality

v). power filters and conditioners

vi). any other matters required by the service provider and as agreed by the Commission.

6 Pre-commitment equipment (hardware)

This chapter sets out the hardware requirements for PCS equipment that must be followed for operation in Victoria.

6.1 Hardware requirements

6.1.1 The design and configuration of all PCS equipment hardware and any changes to PCS equipment hardware must be submitted by the service provider to the Commission for approval.

Information display

6.1.2 Touch screens and keypads used with information displays must meet the technical requirements set out in the Player Account Equipment Technical Requirements document.

Card reading device

6.1.3 Card readers used for identifying players to the PCS equipment must meet the technical requirements set out in the Player Account Equipment Technical Requirements document.

Device I/O

6.1.4 PCS equipment must protect against malfunctions, fraud or invalid results caused by the simultaneous or sequential activation of the various device inputs or outputs.

6.2 Maintenance requirements

6.2.1 Maintenance of PCS equipment that is the responsibility of the service provider is only to be conducted by an organisation(s) that is listed on the Roll of Manufacturers, Suppliers and Testers or is contracted by the service provider.

6.2.2 All scheduled maintenance should be carried out in accordance with a maintenance schedule that has been approved by the Commission.

Retention of data

6.2.3 All equipment statistics, pre-commitment information and metering information stored in the equipment (whether by electronic, magnetic, mechanical or other means) shall be retained during hardware maintenance and shall be protected against damage, destruction or alteration during maintenance operations (including battery replacement).

6.2.4 Maintenance procedures must be such that clearance of 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

6.2.5 Maintenance must be carried out in such a way to not impact on the approval for the system or any of its equipment.

6.2.6 Maintenance or repair of approved equipment must be undertaken using replacement parts that are identical or equivalent to the parts constituting an approved device.

6.2.7 Hardware maintenance of equipment shall not be by any of the following means:

i). testing and fault diagnosis requiring the cutting of electronic circuitry

ii). testing and fault diagnosis requiring the drilling of electronic circuitry

iii). testing and fault diagnosis requiring the addition of electronic circuitry

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.

6.2.8 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

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

7 Pre-commitment equipment (software)

This chapter sets out the software requirements for PCS 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 PCS equipment software and any changes to PCS equipment software used within the PCS, including but not limited to PCS equipment for venues.

7.1.2 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.

7.1.3 All software must meet the software requirements set out in the Commission's Standards.

7.2 Software quality requirements

Source code

7.2.1 The source code for all software components of the PCS must be provided (where possible) to the Commission and/or a tester in an approved machine-readable form. Program and functional documentation must 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

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 PCS 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 service provider 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 service provider but it must strictly follow the service provider'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 service provider and/or suppliers of PCS 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 where the service provider has the capability, right, or access to source to provide (which may be the IP of a third party provider)

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 14, 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 service provider and randomly on demand by the Commission.

vii). There must be a method available to determine if unapproved programs, command files, fixed data files, etc. reside on any component in the PCS.

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.

8 Player account requirements

This chapter sets out the requirements that must be followed for player activities carried out in Victoria.

8.1 Player accounts

8.1.1 Player account activities must only be available to players who are registered with the service provider.

8.2 Creation of player accounts

8.2.1 Only natural persons over the age of 18 years are permitted to register for a player account.

8.2.2 The player must be allocated a unique identifier to enable identification of the appropriate player by the PCS each time a player commences a session.

Registered player account

8.2.3 A registered player may only have one active player account.

8.2.4 A venue operator must carry out a Proof of Identity check for each applicant.

8.2.5 The service provider must securely maintain a register of player accounts.

8.2.6 The PCS must facilitate the cancellation of a player’s profile and re-registration.

Casual player account

8.2.7 The Pre-commitment system must provide access to the pre-commitment services for players who want to remain anonymous.

8.2.8 Casual player account must be accessible via a player card available in all Victorian gaming venues obtained and enabled without assistance from venue staff.

8.2.9 A casual player account might not be able to be cancelled and re-activated.

Non player accounts

8.2.10 The service provider must classify ‘Technician Cards’.

8.2.11 The service provider must classify ‘Venue Manager Cards’.

8.2.12 The service provider must provide Inspectors with ‘Inspector cards’ to enable the Inspectors to perform their role in ensuring that the venue operators and the service provider have met their obligations in providing pre-commitment services to players.

8.2.13 Pre-defined Victorian Government reports and card counts exclude any details relating to the following accounts:

i). technician

ii). venue manager

iii). inspector.

8.3 Privacy of registered player information

8.3.1 Any information obtained by the service provider in respect of player account establishment must be kept confidential by the service provider as required under the pre-commitment related agreement, except where the release of that information is required by law or approved by the registered player.

8.3.2 Any information about the current state of player accounts or player activity must be kept confidential by the service provider except where the release of that information is required by law or approved by the registered player.

8.3.3 Use of registered player information in development, testing and production environments must not breach the Australian Privacy Principles and the *OECD Guidelines on the Protection of Privacy and Transborder Data Flow of Personal Data*[4].

8.3.4 Data management must be in accordance with the *Privacy and Data Protection Act 2014(Victoria)* and the *Privacy Act 1988 (Commonwealth)*.

8.3.5 All registered player information must be erased (that is not just deleted) from hard disks, magnetic tapes, solid-state memory and other devices before the device is decommissioned or sent off-site for repair. If the information on the device cannot be erased, the device must be physically destroyed.

8.4 Player accounts maintenance

8.4.1 Storage of activity data on the PCS must be secured against invalid access or update other than by approved methods.

8.4.2 All adjustment transactions are to be maintained in a system audit log.

8.4.3 All transactions involving player's activity data are to be treated as vital information to be recovered by the PCS in the event of a failure.

8.4.4 Personal information of a sensitive nature must only be kept and stored in an encrypted form in transit and at rest. The encryption must meet cryptographic standards equivalent to the standards set out for encryption in the 'Australian Government Information and Communications Technology Security Manual (ISM) – Controls'.

[4] www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf, viewed 25 February 2015.

8.4.5 In relation to 8.4.4, personal information of a sensitive nature includes, but is not limited to:

i). registered player’s first name

ii). registered player’s last name

iii). registered player’s address (excluding postcode).

8.4.6 The following information must only be stored using an irreversible encryption algorithm:

i). A player’s PIN and password used to access details of their PCS player account.

8.5 Player statements

8.5.1 A player activity statement must be available to the player upon request and/or in compliance with the prescribed requirement.

8.5.2 Player activity statements must include sufficient information to allow the player to reconcile the statement against their own records to the session level.

8.6 Cancelled player accounts

8.6.1 The service provider must establish policies, standards and procedures regarding the treatment of retention of dormant or cancelled accounts.

8.7 Player activity data

8.7.1 The player account dataset must be able to be viewed and managed as a logically distinct dataset.

8.7.2 All player activity database transactions are to be recorded as critical data by the PCS and recovered in case of host failure.

9 Pre-commitment services

This chapter sets out the scope of pre-commitment functional requirements that must be followed for operation in Victoria.

9.1 Common functional requirements

9.1.1 The PCS must provide the necessary functionality in order to allow:

i). players to access the pre-commitment services

i). venue operators to offer pre-commitment and assist players

ii). the service provider to provide and assist players to use pre-commitment

iii). reports to be generated for players, venue operators and the Victorian Government.

9.1.2 The PCS must provide all necessary functions, tools and procedures in order to meet the service delivery requirements set by the Pre-commitment related agreements.

9.2 Access to pre-commitment

Player access

9.2.1 The system must allow the players to access pre-commitment services via the following methods:

i). at the gaming machine upon successful account authentication using pre-commitment card and PIN

ii). online Internet access via a web browser upon successful account authentication of the player's account's credentials: username or email address and password

iii). via venue kiosk upon successful account authentication using pre-commitment card and PIN

iv). via venue kiosk upon successful account authentication of the player's account's credentials: username or email address

v). via the service desk, with the assistance of an operator

vi). at the player service point – with the assistance of venue staff – upon successful account authentication using pre-commitment card and PIN.

Note: player service point devices and kiosks must have online Internet or direct access to the public facing PCS network.

9.2.2 At the gaming machine, the system must only access pre-commitment to track their play. That is, at the gaming machine, the system must not permit players to register for pre-commitment, update personal details and/or update limits.

9.2.3 The system must allow players to reset and enter new PIN via the pre-commitment website, at the kiosk and with the help of the help desk.

9.2.4 The system must allow anonymous players to reset and enter new PIN via the kiosk and via the website if the player enables online access via the kiosk. Anonymous players may not be able to reset and enter their PIN via help desk and player service point due to lack of identification.

Venue operator access

9.2.5 The system must enable the use of a unique login account for each venue's staff members. The system must be accessible to venue staff at the player service point using the venue's staff member's account details.

9.2.6 The system must be able to categorise venue staff accounts as:

i). a member of the venue's PCS management group

or

ii). a member of the venue's PCS venue counter group.

9.2.7 The system must enable the venue staff to perform searches based on search criteria in order to assist the player at the player service point.

9.2.8 The system must not allow venue staff to access players' security information and play-history at the player service point.

9.2.9 The system must allow access to players account at the player service point up on successful validation of the player's card credentials: successful PCS card read and PIN.

9.2.10 The PCS management group has the same functionalities as the PCS venue counter access group, with the additional functionality of accessing PCS venue reports.

Help desk access

9.2.11 The system must enable the service desk operator to perform searches based on search criteria in order to help the registered players to reset their PIN or access their player account upon providing valid identifiable information.

Inspectors

9.2.12 The system must enable the use of a unique login account for each Inspector. The system must be accessible to Inspectors at the player service point using the Inspector's account details.

9.3 Player registration and cancellation

9.3.1 The player must be able to pre-register for accessing pre-commitment services online, at a kiosk, via the help desk or with the assistance of venue staff at the player service point.

9.3.2 The system should meet the player account requirements set in section 8 of this document including the minimum information required at registration.

Registration

9.3.3 At pre-registration the player must be able to update their details and set pre-commitment limits.

9.3.4 A registered player must be able to update their details set pre-commitment limits and modify their personalised alert message, either online, at a kiosk, via the help desk or with the assistance of venue staff at the player service point.

9.3.5 A casual player must be able to reset or change their PIN or password and set pre-commitment limits, online, at a kiosk, via the help desk or with the assistance of venue staff at the player service point.

9.3.6 The system must present and capture players' consent to the terms and conditions and enable venue staff to record that a player's identification document has been sighted during pre-registration.

9.3.7 The system must not retain player's information if that player has not consented to Terms and Conditions.

Pre-commitment card

9.3.8 The registration process completes with player receiving a pre-commitment card issued by the venue operator. The system must

i). allow venue staff to record that player's identification document has been sighted and that it matches details provided at pre-registration

ii). record that the PCS player's card has been issued at the venue.

9.3.9 Pre-encoded pre-commitment cards must be available in all Victorian venues and must allow the anonymous player to access the system without following the registration process.

9.3.10 The system must allow venue staff to encode a standalone or dual player pre-commitment card including additional card with unique pre-commitment ID number. The system must record the venue name and location where the pre-commitment card was issued.

9.3.11 The system must recognise a pre-commitment card issued by one gaming venue when used in any other gaming venue in Victoria.

Cancellation

9.3.12 The system must enable registered players to cancel their pre-commitment account and retain the optional reason for cancellation.

9.3.13 The system must enable players to revert their cancellation within 24 hours of cancellation.

9.3.14 The system must unlink and not be capable of re-linking historical pre-commitment data against the player once the final activity statement has been sent to the player and the prescribed time has expired.

9.3.15 The casual player will not be able to cancel their account unless converted to a registered account.

9.4 Pre-commitment limits

9.4.1 Limit types must be configurable on the PCS, allowing for the removal or addition of limit(s) types. The system must offer the following limit types at minimum:

i). daily, or weekly net loss limit, and/or

ii). daily or weekly time limit

or

iii). no limit.

9.4.2 Net loss equals the cumulative amount bet (in dollars and cents) less the cumulative amount won (in dollars and cents) less jackpots awarded over the limit period. Non-cash jackpots are not included in the net loss.

9.4.3 Time limit equals the cumulative amount of time the player nominates to spend playing gaming machines during the limit period.

9.4.4 In terms of pre-commitment, a limit period is either a day or week, with:

i). a day commencing at 6:00am and concluding 5:59am the following day

ii). a week commencing at 6:00am on a Monday and concluding 5:59am the following Monday.

9.4.5 The Commission has the discretion to introduce a monthly limit option for net loss limit and time limit. With the month period commencing at 6:00am on the first day of the month and concluding 5:59am on the day after the last day of the month.

9.4.6 The methods of calculating the pre-commitment limits and the frequency of updating the current pre-commitment balance per limit must be approved by the Commission.

9.4.7 The updated limit has to apply immediately if the limit is tightened before a limit has been reached. If a limit is loosened after a limit is reached, the new limit applies after a cooling period. The cooling off period must be a configurable parameter on the system. If a pre-commitment card has not been issued, players must be able to update their limit(s) without the system applying the cooling-off period.

9.4.8 The system must enable registered players to set, update and cancel a personalised alert message. A standard alert message will be displayed when limit thresholds are reached together with a player's personalised alert message, if set.

9.4.9 Anonymous accounts will have the default limit set to 'no limit' until the player selects the limit type and amount via kiosk or website as per 9.4.1.

9.4.10 Anonymous player may not be able to set personalised messages. A standard alert message will be displayed when limit thresholds are reached.

9.5 Tracking Play

9.5.1 The system must capture all pre-commitment session data including but not limited to:

i). date/time a session is started

ii). date/time a session is ended

iii). location of the session

iv). date/time a live action summary was requested by the player

v). play activity

vi). any other information as agreed to between the Commission and the service provider.

9.5.2 The system must allow players to use their pre-commitment card at a gaming machine immediately after the pre-commitment card is issued. The system must recognise a pre-commitment card issued by one gaming venue when used in any other gaming venue in Victoria.

9.5.3 The system must start a pre-commitment session upon validating the player's PIN and starts tracking the player gaming activities until end of session when card is removed or gaming non-activity time-out elapsed.

9.5.4 Only one session per pre-commitment account is allowed at any time.

9.5.5 The system must display immediately after the session starts:

i). The limit reached message at the gaming machine immediately after the session starts if the player has either reached a limit or has a zero limit time or net loss limit

or

ii). The live action summary at the gaming machine immediately after the session starts if the player has not reached any of their limits.

9.5.6 The game must be disabled once the player reaches 100 per cent of their current limit or the system determines that zero limit has been set. The game should be allowed to complete before disabled by the system. When the game is disabled, the system must allow money collection.

9.5.7 After the machine is disabled as per 9.5.6 the system must:

i). display a limit reached message (9.4.8)

ii). provide an option for the player to end the pre-commitment session by:

a) removing the card from the gaming machine
or
b) to continue playing within the pre-commitment session after confirmation of their request to continue playing.

9.5.8 After the machine is disabled as per 9.5.6 the game must be re-enabled after the pre-commitment card is removed or the player confirms continuation of game play.

9.5.9 The system must display a live action summary during play at periodic intervals and on player request.

9.5.10 During the session, the pre-commitment system must display on the gaming machine a limit threshold message (9.4.8):

i). if the player has set a net loss limit, when a limit threshold of the player's net loss limit is reached
ii). if the player has set a time limit, when a limit threshold of the player's time limit is reached.

9.5.11 During the session, when the pre-commitment system displays a limit threshold message (9.4.8), the limit threshold message must be closed:

i). by the player's action to close the their limit threshold message
or
ii). the system closes the limit threshold message, after a configurable period.

9.5.12 During the a session, if a limit has been reached at the same time as a limit threshold, then the limit reached message must be displayed instead of the limit threshold message.

9.5.13 The live action summary must display the following information:

i). the total time the player has spent using the gaming machine during the session (as at the time the live action summary is displayed)

ii). the player's net loss during the session (as at the time the live action summary is displayed)

iii). if the player has set a time limit:

a) the player's time limit
b) the cumulative amount of time that has expired over the limit period.

iv). if the player has set a net loss limit:

a) the player's net loss limit
b) the cumulative amount of net loss over the limit period.

v). if the player is continuing play despite having reached a limit or having set a zero dollar net loss and/or zero time limit:

a) a message reminding the player that they are playing beyond their limits.

9.5.14 During a session, when the pre-commitment system displays a live action summary, the live action summary must be closed:

i). by the player's action to close the live action summary, or
ii). the system closes the live action summary, after a configurable period.

9.6 Reporting

9.6.1 The following reports must be made available by the service provider in accordance with and as set in the Pre-commitment related agreement:

i). player annual activity statement. players will be able to obtain this statement either by online, email or by post

ii). player dynamic activity statements. Players will be able to generate the report by online means only.

9.7 System performance

The service provider must comply with the following system performance requirements in an agreed upon controlled environment:

9.7.1 The system must allow log in to the user interface in no more than five seconds upon pressing the 'enter' key at login.

9.7.2 The system must be capable of switching between user interface screens in no more than two seconds.

9.7.3 The system must allow a standard report to be generated in no more than 10 seconds.

9.7.4 The system must allow registration to take no more than two minutes.

9.7.5 The system must respond and return a value on screen within two seconds of pressing a command (for example. via the 'enter' key, mouse or appropriate function key) for simple transactions.

9.7.6 The system must respond and return information on screen within two seconds of inserting the pre-commitment card in the card reader at the gaming machine.

9.7.7 The system must display activity statements within 30 seconds.

9.7.8 The system must detect and advise the player that a limit has been reached within three seconds of game play (except on VLC gaming machines).

10 Integration with loyalty systems

This chapter sets out Pre-commitment system requirements for integration with loyalty system for operation in Victoria.

10.1 Infrastructure and data

The Gambling Regulations Amendment (Pre-commitment) Bill 2013 sets down the following requirements for sharing of equipment between the PCS and a venue's loyalty system:

10.1.1 Loyalty scheme must use same equipment as the PCS as per section 3.5.36D of the Act

10.1.2 The PCS component residing in the loyalty device at the EGM will be signature checked by the PCS.

10.1.3 If the venue has a loyalty scheme, then any of the following PAE installed in a gaming venue must be shared between the loyalty scheme and the PCS:

i). a card reader installed in a gaming machine

ii). an interactive display screen installed in a gaming machine

iii). kiosk(s)

vii). any other prescribed equipment, as agreed to between the Commission, the service provider and the loyalty scheme providers.

10.1.4 The PCS component within the loyalty device must notify the PCS of PAE related significant events.

10.1.5 Pre-commitment data must not be shared with any other ancillary service system. The pre-commitment data can be passed through to the player account equipment in the venue by other devices provided that the data is not stored.

Note: the above includes loyalty applications.

10.1.6 PCS must send a notification to the loyalty system interface when the following events occur:

i). pre-commitment session has timed out
ii). a limit is reached for the first time during a session
iii). player has had three invalid attempts at entering their PCS PIN (account lockout)
iv). timeout to login to pre-commitment has been reached
v). after the PIN validation at the EGM, the system identifies that the player has set a $0 net loss or zero time limit, or
vi). after the PIN validation at the EGM, the system identifies that the player has already reached a limit.

In addition, loyalty point accumulation must cease.

10.1.7 PCS must not affect a registered player's access to the loyalty scheme other than for section 10.1.6.

10.2 Functional requirements

Dual player cards

10.2.1 Players registered for pre-commitment and loyalty at a gaming venue must be allowed to use their dual player card to access pre-commitment.

10.2.2 The system must allow venue staff to encode dual access cards with the player's pre-commitment ID and loyalty scheme ID.

10.2.3 A dual player card must be encoded with pre-commitment ID and a loyalty scheme ID in accordance with the coding convention requirements in 'Victorian Player Account Equipment Technical Requirements'.

10.2.4 If the player has a dual player card, the player can play as a registered player and access the venue's loyalty scheme associated with the card

10.2.5 If the player has a dual player card, the player can play as pre-commitment registered user irrespective of the card's loyalty scheme. This expands on section 9.3.11.

Messaging

10.2.6 PCS messages must be displayed before any loyalty scheme messages or information.

10.2.7 PCS messages must never be displayed at the same time as loyalty scheme messages at an EGM. Only one system can have control of the display at any point in time.

10.2.8 When PCS generates a message to the loyalty scheme, the loyalty system must manage the loyalty scheme's audio at the gaming machine in a manner consistent with the Regulations.

Loyalty points accumulation

10.2.9 The PCS must send a message to the loyalty system to stop point accumulation or prevent the meter feeds to the loyalty system for the conditions specified in section 10.1.6.

10.2.10 Loyalty point accumulation is allowed, in a scenario where the PCS services are not available to the player at the EGM while gaming and loyalty are still available.

11 Network and communications

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

11.1 Communications requirements

Communication scheme

11.1.1 Unless otherwise agreed by the Commission:

i). all communications must be via a protocol based communications scheme

ii). signature verification of all approved baseline software must be initiated and the outcome verified by a separate, higher-level component of the PCS.

Data communications

Protocol

11.1.2 Commission approval must be received in advance for any protocol used for data communications between PCS equipment.

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

11.1.4 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

11.1.5 Communications protocols must include the following:

i). error control

ii). flow control

iii). link control (remote connection).

Error detection

11.1.6 Communications protocols must make use of Security, Authentication and Integrity process (SIA's) or the equivalent.

11.1.7 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.

Communications failure modes and recovery

11.1.8 If the wide area network link between the central site and the gaming venue is lost, the PCS must continue tracking the active pre-commitment session until its completion.

11.1.9 Starting a new pre-commitment session during a link failure is not permitted.

11.1.10 Upon recovery of the link between venue and central, all session data gathered and stored on the venue devices while off-line must be send to central.

11.1.11 All PCS equipment and pre-commitment data must be recoverable to the point of failure following an interruption.

11.1.12 Some typical scenarios which may be tested by the Commission’s representatives at time of system evaluation to ensure compliance of the system failure and recovery processes are:

i). failure of central computer LAN interfaces

ii). failure of LAN

iii). failure of data communication interface devices

iv). Failure of single data communication interface

v). WAN edge network device failure at central

vi). WAN edge network device 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). data communication interface failure on a gaming machine.

11.2 Cryptographic data security

Introduction

11.2.1 Cryptographic data security refers to the protection of critical communication data from eavesdropping and/or illicit alteration.

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

11.2.3 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

11.2.4 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:

iv). signature seeds (algorithm coefficients)

v). signature results

vi). encryption keys, where the implementation chosen requires transmission of keys

vii). PINs

viii). registered player's personal details

ix). passwords.

x). examples of critical data security which would be satisfied by an approved message authentication algorithm include software uploads and downloads of any security related software.

xi). 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

11.2.5 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 128 bits.

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

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

11.2.6 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’ .

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

11.2.7 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.

11.3 Network requirements

General

11.3.1 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 service provider’s system design.

Network baseline

11.3.2 During the approval stage of a system network, and based on the System Baseline Document prepared by the service provider, the Commission will determine the core areas of the system network for which verification control must be maintained. The control and security measures of the core systems network is defined and approved in a Network Policy Document. This document is the responsibility of the service provider to prepare as part of its submission to the Commission when obtaining approval for the PCS. This document must describe the network topology of the system detailing the interconnection of modules with and within the core network and the types of connections permitted.

Physical requirements

11.3.3 Power to devices inside and on the boundary of the baseline envelope must be provided from a filtered, dedicated power circuit.

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

Network documentation

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

11.3.6 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

11.3.7 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.

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

11.3.9 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.

11.3.10 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.

11.3.11 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

11.3.12 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 per cent.

11.3.13 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.

11.3.14 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

11.3.15 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 service provider. Note that WAN communication links will be generally deemed to be outside a baseline envelope.

11.3.16 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 per cent.

11.3.17 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.

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

11.3.19 Communication between devices in separate baseline envelopes must be immune from ‘man-in-the-middle’ attacks.

Communications to devices outside a baseline envelope (firewall)

11.3.20 Data exchanged with computer systems and terminals outside the baseline envelope must pass through at least one network control device (for example router or firewall). The network control devices must implement the controls as defined in the network policy document, which must be prepared by the service provider and submitted to the Commission for approval.

11.3.21 The network control devices involved in implementing the network policy document must be located at the boundary or inside the baseline envelope.

11.3.22 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.

11.3.23 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.

11.3.24 Computer systems within the baseline envelope must not be affected by network attacks emanating from outside the baseline envelope (for example ping-of-death attacks, teardrop attacks, routing protocol attacks, etc.).

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

11.3.26 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 PCS pertaining to the transfer (date, time, person account or system account, and file(s) transferred)

ix). immunity from man-in-the-middle attacks

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

Host monitoring systems and network management systems

11.3.27 Evaluation must be performed and approval obtained, if required for host monitoring systems that monitor hosts inside or on the boundary of a baseline envelope.

11.3.28 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.

11.3.29 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.

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

i). imitating the IP address of a host monitoring system or a network management system

ii). imitating the hardware address (for example Ethernet address) of a host monitoring system or a network management system

or

iii). replaying previously captured communications.

11.3.31 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

ii). imitating the hardware address (for example Ethernet address) of a host monitoring system or a network management system

or

iii). replaying previously captured communications.

Internet connections

11.3.32 Internet connections must demonstrate adequate network-based and host-based intrusion detection capabilities, and must include automatic alerts in the event that a security breach occurs and/or the detection of unsuccessful attacks on the system.

11.3.33 The PCS, at the point where it is connected to the Internet service provider, must incorporate secure type of architecture.

11.3.34 The internal and external firewalls must be of a type to ensure that any weakness in one firewall structure is not duplicated in any other firewall.

11.3.35 The service provider must have the ability to terminate a remote customer's session.

Verification tools

11.3.36 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.

11.4 Wireless communication

11.4.1 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) – Controls', to overcome the general weaknesses of wireless communication,

11.4.2 Wireless communication will be considered for local area network communications within venues and/or wide area network communication between venues and the host PCS.

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

11.4.4 The access point must not be placed directly onto the venue network unless a stand-alone stateful packet inspection firewall is employed.

11.4.5 Wireless network traffic must be secured with additional encryption and/or authentication codes and must meet the requirements of section 11.2.5.

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

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

12 Pre-commitment significant events

This chapter sets out pre-commitment significant events requirements that must be followed for operation in Victoria.

12.1 General

12.1.1 This section is a summary of each of the PCS significant events that are required, including the type of event.

12.1.2 The following list defines one type of significant event and the 'type' numbers used refer to this list:

i). **TYPE 6:** Information Only (no de-activation of PCS or CMCS components)

12.1.3 Reporting on the status changes of the following PAE components are optional:

i). display screen at the EGM

ii). venue kiosks

iii). service desk components connected to the venue network.

Note: Commission monitors significant events at its premises and that each significant event will be tested during the formal acceptance tests.

12.1.4 The Pre-commitment system has to maintain an audit log of significant events. At minimum, the access audit log must contain at least:

i). when the event occurred: date timestamp of the significant event

ii). location of the event: such as venue identifier and device.

12.2 Significant events

The following are the significant events that are determined by the PCS:

PCS equipment or PAE communication failure

12.2.1 The PCS detects the failure of a PCS or PAE component to respond to a handshake command. The requirement applies to link failure with the PCS host. A record of this failure must be logged in an audit file and recorded as a significant event.

PCS or PAE communication recovery

12.2.2 The PCS detects the recovery of PCS or PAE equipment communication after communication failure. A record of this event is to be logged in an audit file and recorded as a significant event.

Limit reached

12.2.3 The PCS determines that a player has reached or exceeded a pre-commitment limit and accordingly has instructed the gaming machine to disable the game. The PCS must ensure that the gaming machine remains de-activated until the player's card is removed or player confirms continuation of play. A record of this event is to be logged in an audit file and recorded as a significant event.

Signature failure

12.2.4 The PCS determines that a component of equipment has failed a signature check. A record of this failure must be logged in an audit file and recorded as a significant event.

Pre-commitment service not available

12.2.5 The PCS determines that the pre-commitment services are not available for the Victorian Government, at the venue or at individual EGMs due to device failure or pre-commitment disable function executed by the PCS system operator. A record of this event must be logged in an audit file and recorded as a significant event.

Pre-commitment service recovered

12.2.6 The PCS determines that the pre-commitment services are recovered and available at venue or at EGMs after device failure or after being enabled by the PCS system operator. A record of this event must be logged in an audit file and recorded as a significant event.

13 Submission requirements

This chapter sets out the submission requirements for evaluation in Victoria. It primarily applies to the service provider's pre-commitment system and pre-commitment equipment.

13.1 General

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

i). background of the PCS

ii). purpose of the submission

iii). description of the scope of system and operational changes

iv). tester recommendation of the PCS in accordance with above requirements

v). the service provider's comments on any conditions included in the tester recommendation

vi). list of all software versions and associated SIAs

vii). list of all relevant hardware and operating systems – product names, models and versions

viii). associated systems that are connected to the PCS

ix). a PCS Baseline Document

x). a Network Policy Document.

Environmental testing

13.1.2 Suppliers of PCS equipment are to provide information as to the range of environmental extremes at which PCS 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.

13.1.3 The Commission requires the equipment to run within the equipment's own environmental specifications.

13.2 PCS/Site operator requirements

13.2.1 The Commission must be satisfied that all procedures pertaining to the requirements of section 5 have been addressed. To this end, the service provider 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.

13.3 Player information

13.3.1 The service provider must provide player registration process details.

13.3.2 The service provider must provide descriptions of how player verification information is to be protected from unauthorised access.

13.3.3 The service provider must provide details of player authentication.

13.3.4 The service provider must provide details of the player limit mechanisms.

13.3.5 The service provider must provide descriptions of how player registration and account information is to be protected from unauthorised access.

13.4 Communications

Authentication and encryption

13.4.1 The service provider must provide details of the message authentication algorithm used.

13.4.2 The service provider must provide details of the encryption to be used:

i). encryption algorithms

ii). size of encryption keys

iii). key exchange procedure at session start-up

iv). subsequent key exchanges

v). details of any information that is not encrypted for transmission.

PCS internal network architecture

13.4.3 The service provider must provide details of the proposed architecture of the internal production network to be used to supply pre-commitment scheme facilities:

i). network topology

ii). devices used to create the network

iii). controls to prevent unauthorised modification to device configuration.

13.4.4 The service provider must provide a description of the details of connections to the Internet.

13.4.5 The service provider must provide details of any remote connections (for example Internet, wide area network, and dial-up) used to support Pre-commitment Scheme operations.

13.4.6 The service provider must provide details of authentication and encryption associated with remote connections.

13.4.7 The service provider must provide details of operator consoles, including:

i). location of operator consoles in relation to the PCS

ii). protocols used by operator console connections

iii). access controls on operator console connections to the PCS

iv). authentication and encryption used by operator consoles

v). controls to prevent eavesdropping on communications between operator consoles and the PCS

vi). controls to prevent unauthorised use of operator consoles.

13.4.8 The service provider must provide a list of all non-baseline systems, non-production systems and third party systems that will connect to the PCS.

13.4.9 For each external system provided in relation to 13.4.8, the service provider must provide:

i). the connection method

ii). details of the information to be transferred in each direction

iii). the entity that initiates the information transfer

iv). the protocol used to perform the transfer

v). the controls in place to prevent access to other information on the PCS

vi). the controls in place to prevent unauthorised use of the connection

vii). the controls in place to prevent eavesdropping on communications between non-production systems and the PCS.

13.4.10 The service provider must provide details and configurations of the devices that will be used to control access from the Internet to the internal production network (including authentication and encryption).

13.4.11 The service provider must provide details and configurations of the devices that will be used to control access from other networks (including non-production networks used by the operator) to the internal production network.

13.4.12 The service provider must provide details of controls and audit trails associated with access and modifications to network components.

13.4.13 The service provider must provide details of any network management system associated with the internal production network, including:

i). the physical location of the network management system

ii). the class of personnel authorised to use network management system

iii). the locations from where network management functions can be executed

iv). the network management protocol

v). the devices to be managed on a read only basis vi). the devices to be managed on a read/write basis

vii). the controls in place to prevent unauthorised access to network management functions

viii). the controls in place to audit the use of network management functions

ix). the controls in place to detect unauthorised connections to the network

x). the controls in place to detect connection of unauthorised equipment to the network.

13.4.14 The service provider must provide descriptions of the locations and physical and logical security arrangements associated with domain name servers within the internal production network.

Third party connections

13.4.15 The service provider must provide description details of all connections to third party organisations.

PCS host computers

13.4.16 The service provider must provide an overview of the PCS design.

13.4.17 The service provider must provide a functional specification of the PCS.

13.4.18 The service provider must provide detailed PCS design documents.

13.4.19 The service provider must provide details of all computer systems used by the PCS including, but not limited to:

i). hardware platform

ii). operating system

iii). applications

iv). audit subsystem

v). duplication strategy

vi). disk subsystem

vii). magnetic back-up facilities

viii). physical security

ix). login security

x). power requirements

xi). environmental condition requirements.

13.4.20 The information requested in relation to 13.4.19 applies also to other PCS equipment to be used in the PCS computer environment. This should include such devices as:

i). front ends

ii). firewalls

iii). operator consoles (local and remote)

iv). remote controllers

v). remote access servers

vi). multiplexing equipment

vii). switching equipment

viii). monitoring equipment

ix). routers

x). repeaters.

13.4.21 For each PCS component and associated equipment that is to be implemented, the service provider must provide a detailed schedule of the planned implementation. This should include dates for the following:

i). first access to the PCS computer system

ii). access to the ‘final’ PCS computer system

iii). first access to each piece of individual equipment

iv). final access to each piece of individual equipment

v). expected date when the service provider's testing and quality assurance has been completed and formal acceptance testing might begin

vi). planned date for live operation.

13.4.22 The service provider must provide descriptions of where and how information is stored throughout the system.

13.4.23 The service provider must provide what statistics are stored by the system.

13.4.24 The service provider must provide detailed descriptions of its password protection systems and associated algorithms utilised by the system.

13.4.25 The service provider must provide a description of the method of transaction logging used.

13.4.26 The service provider must provide details explanations of the situations during which encryption of data files will be employed.

13.4.27 Where data files encryption is to be employed, the service provider must provide the following information:

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

v). means of setting and protecting keys.

13.4.28 The service provider must provide a description on how self-monitoring is to be implemented.

PCS software

13.4.29 The service provider must provide the source software for PCS software.

13.4.30 The service provider must provide a description of how the each of the seven points for software verification detailed in 7.2.11 is to be achieved.

13.4.31 The service provider must provide a description of the method to be used to verify the integrity of the software operating on the production PCS.

PCS operations

13.4.32 The service provider must provide details of each class of account required to operate the PCS in a production environment (for example system administrator, operator, hotline, network support).

13.4.33 For each class of account provided in relation to 13.4.32, the service provider must provide details of the privileges required to perform the duties associated with that account.

13.4.34 The service provider must provide details of the physical location of each component of the PCS, including the location of staff.

13.4.35 The service provider must provide PCS operators manuals, operator’s procedures manuals and system administrator manuals or equivalent.

13.4.36 The service provider must provide copies of all standard reports produced by the PCS and describe how these are generated.

14 Testing requirements

This chapter sets out the PCS testing requirements that must be followed for operation in Victoria.

14.1 Inspection and testing

14.1.1 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.

14.1.2 The service provider must establish and maintain policies, procedures and standards for quality assurance[5] 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)[6] 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

xi). business readiness, including provision for a live trial when required by the Commission.

14.1.3 The service provider’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.

[5] The methods an organisation puts in place to ensure reliable quality control.

[6] An international community where member organisations, full-time staff, and the public work together to develop Web standards. (www.w3.org)

Tester evaluation

14.1.4 The tester will work with the service provider to undertake an evaluation of the proposed pre-commitment system to ensure it meets the requirements set out in the pre-commitment related agreements as well as relevant Technical Standards.

14.1.5 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

iv). system baseline and network security policy document for future approval.

Facilities for a tester

14.1.6 The service provider must make the appropriate facilities available to a tester in the course of the service provider'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

14.1.7 The service provider must ensure that upgrades to the PCS and associated PCS 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.

14.1.8 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.

14.1.9 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.

14.1.10 The test system must be able to interface to venues in a wide range of geographical areas.

Failure modes and recovery testing

14.1.11 The service provider must ensure that a tester is able to test the host PCS for resilience, recoverability and continuity of service, including but not limited to conditions for:

i). failure of host PCS power supply

ii). total power failure of the host PCS site:

iii). for a short period (for example 30 seconds)

iv). for a long period (for example 30 minutes)

v). verifying there is no single point of failure

vi). individual server capability to sustain persistent load

vii). guaranteed messaging

viii). failure of critical components, including but not limited to processors, handlers, gateways, API's, and communication protocols or similar

ix). failure of critical storage devices, including those holding data files and databases critical to the operation

x). failure of host PCS I/O channels

xi). failure of links with remote interface points

xii). host PCS operator error, including but not limited to invalid data entry.

14.2 System testing requirements

Testing requirements and tester recommendation

14.2.1 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.

14.2.2 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

iv). the system baseline document and network security policy document for future approval.

Associated systems requirements

14.2.3 All the systems associated with the PCS are required to be tested for reliability in processing and delivering all transactions for the PCS.

14.2.4 There must be adequate security arrangements and controls between the approved PCS and the associated systems, and these arrangements and controls must form part of the independent assessment and tester's recommendation.

15 Document information

15.1 Document details

Criteria	Details
Document title:	Victorian Pre-commitment System Requirements document
Document owner:	Victorian Commission for Gambling and Liquor Regulation
Document author:	Pre-commitment Implementation Project, OLGR, Department of Justice & Regulation

15.2 Version control

Version	Date	Description	Author
V1.0	February 2015	Public Release	OLGR, Department of Justice & Regulation

15.3 Approvals

Name	Position	Function
Commission	The VCGLR Commission	Approve

16 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 Player Account Equipment Technical Requirements	December 2014
Commission Standards	Refer Glossary
Australian Government Information and Communications Technology Security Manual (ISM) – Controls	V2014
Victorian Government – Website Management Framework: Accessibility	July 2011 (v3.1)

17 Appendix A - Venue operator requirements

This Appendix sets out the requirements for venue operators in relation to the PCS implemented by the service provider.

17.1 General

17.1.1 It is the venue operator's responsibility to ensure all information relating to registered players is maintained in a manner compliant with the *Privacy and Data Protection Act 2014(Victoria)* and the *Privacy Act 1988 (Commonwealth).*

17.1.2 It is the venue operator's responsibility to have installed and maintained all player account equipment and venue signage.

17.1.3 Any third party gaming systems are also ultimately the responsibility of the venue operator.

17.1.4 It is the venue operator's responsibility to:

i). process and correct potential security breaches as advised by either significant events, the Commission, the service provider or the PCS

ii). ensure each EGM has the capacity to connect to, and operate in accordance with, the PCS, including the fitting and operational status of gaming machine generic equipment as specified in the Player Account Equipment Technical Requirements.

iii). ensure the venue has the capacity to connect to, and operate in accordance with, the PCS, including the installation and operational status of player service point device(s) and kiosk(s) as specified in the Player Account Equipment Technical Requirements

iv). ensure that that the venue's kiosks and player service point device(s) connect to the venue's own network

v). expose the venue's kiosks and player service point device(s) to online Internet or direct access to the public facing PCS network

vi). provide technical assistance on request from the Commission to assist VCGLR Inspector's in the conduct of technical compliance

vii). meet certain standards in providing pre-commitment services

viii). meet any additional requirements required to be included in their Responsible Gambling Code of Conduct.