

Victorian Commission for Gambling and Liquor Regulation

# The Technical Requirements Document for Melbourne Casino



Victorian Commission for  
Gambling and Liquor Regulation





© Victorian Commission for Gambling and Liquor Regulation (VCGLR) - 1993, 1995, 2020

Version 4.06

This report contains commercially confidential and security sensitive information and is not to be released to any individual or organisation without the express written permission of the Victorian Commission for Gambling and Liquor Regulation (VCGLR).

## Contents

<b>1</b>	<b>Introduction</b>	<b>8</b>
1.1	General Information	8
1.2	Objectives	8
1.3	Terminology	8
1.4	Regularity of Interpretation	9
<b>2</b>	<b>Baseline and the Regulatory Definitions</b>	<b>10</b>
2.1	Baseline Components	10
2.2	First Tier Non-Baseline Components	10
2.3	Second Tier Non-Baseline Components	10
<b>3</b>	<b>Technical requirements</b>	<b>12</b>
3.1	Physical Security	12
3.2	Banknote acceptance security	13
3.3	Physical Integrity	14
3.4	Interference	14
3.5	Information Display	14
3.6	Cash Input Systems	14
3.7	Events and Conditions	15
3.8	Notification of Faults	19
3.9	Data Retention	19
3.10	Hashing Algorithm	20
3.11	Critical Memory	20
3.12	PSD Integrity	21
3.13	RAM Clear	21
3.14	PSD Security	21
3.15	Meters and Data	21
3.16	Self-Audit Error Checking	22
3.17	Test or Diagnostic Mode	22
3.18	Configuration	23
3.19	Audit Mode	23
3.20	Random Number Generator and Symbol Selection	24
3.21	Probability	25
3.22	Standard Deviation	26
3.23	Access Detection	26
3.24	Master Meters	26
3.25	Definition of Software Meters	28
3.26	Printed Tickets	29
<b>4</b>	<b>Gaming equipment monitoring and control</b>	<b>30</b>

4.1	Configuration Requirements.....	30
4.2	Game Verification .....	30
4.3	Metering.....	31
4.4	Exception Reporting.....	31
4.5	Functionality.....	32
4.6	System requirements .....	32
4.6.1	Server .....	32
4.6.2	Interface.....	32
4.7	Security requirements .....	33
4.7.1	System Requirements .....	33
4.7.2	CMS Recovery .....	34
4.7.3	Time Synchronization .....	35
4.7.4	Duplication.....	35
4.7.5	Development System .....	35
4.7.6	Data Retention.....	35
4.7.7	Code Download Requirements .....	36
4.7.8	System Integrity.....	36
4.7.9	Events.....	36
4.7.10	Communications.....	37
4.8	Reporting Requirements .....	37
4.9	Voucher In/Voucher Out.....	38
4.9.1	General.....	38
4.9.2	Voucher Types Supported.....	38
4.9.3	Ticket/Voucher Redemption .....	38
4.9.4	Ticket/Voucher Issuance .....	39
4.9.5	Ticket/Voucher System Requirements .....	39
4.10	Cashless Systems .....	40
4.10.1	General.....	40
4.10.2	Player Identification Methods .....	40
4.10.3	Types of Players.....	40
4.10.4	Player Funds .....	41
4.10.5	Cashless System Requirements .....	42
4.10.6	Reportable Events.....	42
4.10.7	Display Requirements .....	43
4.11	Cash Redemption Terminals (CRT) .....	43
4.11.1	Purpose .....	43
4.11.2	Introduction.....	43
4.11.3	Hardware Requirements.....	43
4.11.4	Software Requirements.....	44
4.11.5	Artwork Requirements.....	45

<b>5</b>	<b>Jackpots .....</b>	<b>46</b>
5.1	Jackpot Types.....	46
5.1.1	Deterministic Jackpot .....	46
5.1.2	Non- Deterministic Jackpot .....	46
5.1.3	Standalone Progressive Jackpot.....	46
5.1.4	Linked Jackpot.....	46
5.1.5	Time Based Jackpots .....	46
5.1.6	Card Based Jackpots .....	46
5.1.7	Tournament Jackpot.....	46
5.1.8	Community Jackpot.....	46
5.1.9	External Jackpot system.....	47
5.1.10	Internal Jackpot system.....	47
5.1.11	Communication Failure.....	47
5.2	Mystery Jackpots .....	47
5.2.1	Jackpot Contributions .....	47
5.2.2	Unreasonable Meter Increment.....	47
5.2.3	Jackpot Probability .....	48
5.2.4	Mystery Jackpot Win .....	48
5.2.5	Walk - Away.....	48
5.2.6	Internal Linked Mystery Jackpots .....	48
5.2.7	Parameter Change .....	49
5.3	Progressive Jackpots.....	49
5.3.1	Jackpot Contributions .....	49
5.3.2	Unreasonable Meter Increment.....	49
5.3.3	Simultaneous Wins.....	50
5.3.4	Jackpot Wins When Communications Go Down.....	50
5.3.5	Internal Link Progressives .....	50
5.3.6	Parameter Change .....	50
5.4	Jackpot controller requirements .....	50
5.4.1	General.....	51
5.4.2	Physical .....	51
5.4.3	Critical Memory.....	51
5.4.4	Monitoring of Credits Bet.....	51
5.4.5	Jackpot Configuration.....	51
5.4.6	Error Conditions.....	52
5.4.7	Meter Rollover .....	52
5.4.8	Program Interruption and Resumption .....	52
5.4.9	Independent Software Verification .....	52
5.4.10	Interface to CMS.....	52
5.4.11	Signature Verification .....	52
5.4.12	Jackpot Display .....	52

5.4.13	Jackpot Win .....	53
5.4.14	Jackpot Shutdown .....	54
5.4.15	Reporting Requirements.....	54
5.4.16	Time Synchronization .....	54
5.5	Tournament Jackpots .....	54
5.5.1	Activation of Tournament Mode .....	54
5.5.2	During Tournament Mode .....	55
5.5.3	Submission Requirements .....	55
5.6	Community Style Jackpots.....	55
5.7	Communications .....	56
5.7.1	Between Jackpot Controller and Electronic Gaming Machines .....	56
5.7.2	Between Jackpot Controller and Jackpot Display .....	56
<b>6</b>	<b>Table game requirements .....</b>	<b>57</b>
6.1	Electronic Table Game requirements .....	57
6.1.1	Common Requirements.....	57
6.1.2	System Requirements .....	60
6.1.3	System Security.....	60
6.1.4	Multi-Games .....	61
6.1.5	Communication Protocol .....	61
6.1.6	FATG Requirements.....	61
6.1.7	SATG Requirements .....	63
6.2	Non – Electronic Table Game requirements.....	63
6.2.1	System Requirements .....	63
6.2.2	Table Interface Devices Requirements .....	63
6.2.3	Jackpot Systems .....	63
6.2.4	Display Units.....	64
6.2.5	Communication Protocol .....	64
<b>7</b>	<b>Player Promotion / Bonusing System.....</b>	<b>65</b>
7.1	Overview.....	65
7.2	Player Promotion Systems.....	65
7.3	Bonusing Systems .....	65
7.4	Player Promotion System Requirements.....	66
7.4.1	Player Information Privacy .....	66
7.4.2	Player accounts maintenance .....	66
7.4.3	Database Security .....	66
7.4.4	Display Notification .....	66
7.4.5	Player promotion Account Error Condition.....	66
7.4.6	System Requirements .....	67
7.5	Player bonusing System Requirements .....	67
7.5.1	Database Security .....	67

7.5.2	Display Notification .....	67
7.5.3	System Requirements .....	67
<b>8</b>	<b>Network and Communication Requirements .....</b>	<b>69</b>
8.1	Cryptographic Data Security .....	69
8.1.1	Introduction.....	69
8.1.2	Requirement for Cryptographic Data Security .....	69
8.1.3	Encryption Algorithm.....	69
8.1.4	Message Authentication Algorithm .....	69
8.1.5	Encryption Keys.....	69
8.2	Communications Requirements .....	70
8.2.1	Data Communications Protocol .....	70
8.3	Network Requirements.....	70
8.3.1	Network Policy Document (NPD) .....	70
8.3.2	Physical Requirements.....	70
8.3.3	Network Documentation .....	70
8.3.4	Connection of External Devices to Networks within a Baseline Envelope.....	70
8.3.5	Communications within a Baseline Envelope .....	71
8.3.6	Communications between Separate Baseline Envelopes.....	71
8.3.7	Communications to Devices outside a Baseline Envelope (Firewall) .....	71
8.3.8	Computer Monitoring Systems and Network Management Systems.....	72
8.3.9	Verification Tools .....	72
<b>9</b>	<b>Submission Requirements.....</b>	<b>73</b>
9.1	Introduction .....	73
9.2	New CMS component .....	73
9.2.1	General.....	73
9.2.2	Player information.....	73
9.2.3	Communications.....	73
9.2.4	CMS Infrastructure .....	74
9.2.5	CMS software .....	75
9.2.6	Random Number Generator.....	76
9.3	Updated CMS component.....	76
9.3.1	General.....	76
<b>10</b>	<b>Other CMS Requirements .....</b>	<b>77</b>
10.1	Approval and Notification Requirements .....	77
10.2	Storage Area Policy Document (SAPD) .....	77
10.3	Audit, Verification and Control.....	77
10.4	Cloud Computing .....	77
<b>11</b>	<b>Glossery of Terms .....</b>	<b>78</b>

## 1 Introduction

### 1.1 General Information

1. This Technical Requirements Document contains the system related requirements for the Monitoring System, Jackpot Systems, Table Games, Bonuses & Promotions and related gaming equipment submissions for operation in the Melbourne Casino.
2. The requirements specified in this document are supplementary and do not take the place of any requirements of the prevailing legislation, Licence and related Agreement(s), Rules and Directions.
3. This document must be read in conjunction with the License and Related Agreements, legislative requirements, Rules and Directions.
4. This document will be used by the Licensee and a Tester to test and evaluate the system for compliance, or to test and evaluate changes to a previously approved system.
5. This document will be used by the VCGLR to evaluate compliance by the licensee with the Casino Licence and related Agreement(s) and to evaluate changes to previously approved CMS, in accordance with prevailing legislation. In the event, and to the extent of any inconsistency between the requirements specified in this document, the legislation, Licence and related Agreement, the legislation and or the Licence and related Agreement (including any conditions) will prevail.
6. Copying or reproducing this document (or part of this document) for commercial gain, without prior permission is prohibited.
7. Electronic Gaming Machines (EGM) and games shall comply with the current version of the Gaming Machine National Standards.

### 1.2 Objectives

The intent of this document is to specify sufficient requirements and controls to ensure that operation of the CMS occurs in a manner that is:

1. Fair;
2. Secure;
3. Reliable;
4. Auditable;
5. Supports responsible gaming; and
6. All parties receive their correct entitlement.

It is not the intent of this document to unreasonably:

1. Mandate a single solution or method of realizing an objective;
2. Limit technology;
3. Limit creativity or variety of choice;
4. Limit marketability;
5. Advantage any supplier or manufacturer of equipment; or
6. Preclude research and development into new technology, equipment or innovative solutions. Hence, this document specifies the minimum technical requirements for CMS. This document does not purport to mandate a particular solution or method as the means to realize the requirement.

### 1.3 Terminology

The following terminologies used in this document are to be interpreted as follow:

**Must:** The guideline defined is a mandatory requirement, and therefore must be complied with;

**Shall:** The guideline defined is a mandatory requirement, and therefore must be complied with;



**Should:** The guideline defined is a recommended requirement. Non-compliance shall be documented and approved by the management. Where appropriate compensating controls shall be implemented; and

**May:** The guideline defined is an optional requirement. The implementation of this guideline is determined by the Casino Operator's environmental requirements.

#### 1.4 Regularity of Interpretation

VCGLR acknowledges that the technical standards may be subject to different interpretations by CMS manufacturers, gaming operators and testing laboratories. Alternative interpretations must be referred to the VCGLR for clarifications.

## 2 Baseline and the Regulatory Definitions

The Central Monitoring System (CMS) consists of any component (hardware or software) that enable the CMS to operate in a secure environment and meet the legislative requirements and the licensee's obligations under the relevant License they hold.

The Victorian Commission for Gambling and Liquor Regulation (VCGLR) defines the components of the CMS into the following categories, each with differing regulatory requirements:

### 2.1 Baseline Components

Software and hardware (minimum system requirements where applicable) of the gaming systems, gaming interface devices and any other components that are core to the operations of the system and delivering the gaming environment as outlined in various sections of this document, including but not limited to:

- Operations and monitoring of all electronic gaming activities and devices, and related transactions to and from the devices;
- Any associated system-based gaming activity, such as TITO, cashless gaming systems, jackpots and the player promotions / bonusing system;
- Operation of system based responsible gaming services (such as player pre-commitment);
- Signature computation or version verification of the system-based gaming devices;
- Random number generation, metering, audit logs and significant events where these items are in relation to gaming activities and system-based devices;
- Functions required by regulatory and/or government bodies;
- Primary source of storing data in relation to the gaming activities, and
- Structured reporting only from the primary data source utilised in relation to the ongoing monitoring of gaming activities.

### 2.2 First Tier Non-Baseline Components

Software and hardware that are directly interfacing with baseline components.

### 2.3 Second Tier Non-Baseline Components

Software and hardware that are not directly interfacing with the baseline components but may impact on baseline components.


The VCGLR must maintain ongoing visibility of the end to end CMS, including all components outlined above.

A Licensee must ensure that any additions or deletions to the CMS components are appropriately classified into one of the abovementioned categories, and the appropriate regulatory response is initiated, i.e.; approval of baselined components or notification of a new First Tier non-baseline components.

It is recommended that if the classification in relation to any changes to the CMS is contentious, the Licensee should actively consult with the VCGLR, prior to development and/or implementation of the changes, to ensure the correct classification is made and the appropriate regulatory action is initiated.

Should the Licensee seek the VCGLR's advice on the appropriate classification of any changes to the CMS, the VCGLR may seek that a report from an Authorised Testing Facility (ATF) is provided to support the request, and certifies the classification made by the Licensee.

If deemed that the Licensee has incorrectly classified any changes to the CMS, the VCGLR could instruct the Licensee to reclassify the change which may require further development, cost



and rework by the Licensee. Further action may also be considered for operating an unapproved system should the Commission determined that components should have been baselined and therefore subject to regulatory approval before operating.



### 3 Technical requirements

This section defines general technical requirements for gaming equipment, excluding the approval of electronic gaming machines, used in the conduct of gaming at the Melbourne Casino. All requirements in this section of this document may not be applicable to all gaming equipment. The ATF will determine the specific requirements in this section that will apply to the specific piece of gaming equipment, and ensure the equipment is compliant with these and other applicable standards.

Where necessary, the VCGLR can be contacted for clarification in relation to defining gaming equipment and applicable requirements of this section of this document that will apply.

#### 3.1 Physical Security

1. Gaming equipment shall be manufactured of materials that are suitable for allowing only legitimate access to the inside of the cabinet, (e.g. doors and their associated hinges shall be capable of withstanding determined illegal efforts to gain access to the inside of the gaming equipment and leave evidence of tampering if an illegal entry is made) accessible areas of a cabinet do not have the potential to cause injury and the door of a locked area must be designed to resist the entry of objects.
2. The entirety of a gaming equipment which does not form part of the player's input interface (e.g. buttons) must be stored within one or more locked areas of the gaming equipment. These locked areas must be equipped with door access detection devices (with the exception of areas which have access to lighting only).
3. Access to a locked area 'A', must not be possible from another locked area 'B' without the use of a key for locked area 'A' or without causing undue damage to the gaming equipment.
4. Door access sensors must detect all door openings and closings; and provide applicable feedback to the gaming equipment software.
5. It must not be possible to insert a device into the gaming equipment that will permit external manipulation of any aspect of the gaming equipment when the device's door is shut without leaving evidence of tampering.
6. Liquid spills applied to the outside of a gaming equipment must not affect player interface or the integrity of the device or information stored inside the cabinet or affect the safety of the patrons or staff operating the equipment.
7. If a door access detection system is disconnected (including the cashbox), the gaming equipment must interpret this action as the door being opened.
8. It must not be possible to access the CPU data bus, address bus or CPU control lines without gaining access to the logic area.
9. Electronic components / items that are required to be housed in one or more logic areas are:
  - (a) CPUs and other electronic components involved in the operation and calculation of game play (e.g. game controller electronics, and components housing the game or system firmware program storage media);
  - (b) electronics involved in the operation and calculation of game result determination;
  - (c) electronics involved in the calculation of game display, and components housing display program storage media (passive display equipment exempted);
  - (d) communication controller electronics, and components housing the communication program storage media;
  - (e) interfaces and drivers for metering systems; and
  - (f) all devices that affect the game play function of the gaming equipment.
10. Logic areas shall be fitted with door access detection systems that shall enable software to detect whether the logic door is open or closed regardless of whether mains power is switched on or off (and it shall detect and store information of a logic door open event with the mains power off for at least 14 days). See *Table 2: Gaming Equipment Open/Close Definitions*.

Note: If the logic door is opened more than once while off-line or powered off, it is only necessary for the gaming equipment to treat this as a single entry.

11. Provision must be made for a seal on the logic area as required.

### 3.2 Banknote acceptance security

1. The banknote input system must be constructed in a manner that protects against vandalism, abuse or fraudulent activity. As a guide the following should be addressed:
  - (a) ability to prevent manipulation by the insertion of foreign objects into the banknote input system;
  - (b) ability to deliver a banknote to the banknote storage area (e.g. receptacle), and
  - (c) it must not be possible to disable any validation feature
2. The banknote storage area (e.g. receptacle) is to be attached to the gaming equipment in such a manner so that it cannot be easily removed by physical force. It must be internally located within the gaming equipment (i.e. not attached to the outside). The relevant Jurisdiction may grant dispensation to this requirement if it can be demonstrated that an externally attached banknote acceptor demonstrates at least the same degree of security as one located inside the gaming equipment. Areas of security that will be examined when considering such a dispensation are:
  - (a) physical strength of the attached banknote acceptor device;
  - (b) position of screws, nuts and bolts; and
  - (c) ability to withstand exposure to burning materials such as lighters, matches, ash etc.
3. A banknote acceptor device must be implemented with a means to enable or disable particular value banknotes. The procedure for setting acceptable banknote values must be via a command from the CMCS or access to a secure area of the gaming equipment. If permanent artwork is used to display the acceptable denominations, the latter method which requires attending each gaming equipment is preferred.
4. Banknote acceptors are to be factory set only; it must not be possible to access or conduct maintenance or adjustments in the field, other than:
  - a) the selection of banknotes and limits as defined in this document; or
  - b) changing of approved PSDs or downloading of approved software.
5. The adjustment of the tolerance level for accepting banknotes of varying quality, or the alteration of any of the possible checking procedures is prohibited in the field. If a reader has multiple tolerance levels then the ability to switch to lower levels is to be disabled.

#### Signature Requirements on Distributed Processing

6. There must be some means whereby software associated with the banknote acceptor is able to be verified by a secure signature checking method.

#### Banknote Acceptor Self-Test

7. If the signature requirement is to be met by the self-checking method, evidence is to be provided by the banknote acceptor supplier that the self-check is performed, and details of checks performed.
8. The banknote acceptor device must perform a self-test at each power up. In the event of a self-test failure, the banknote acceptor must automatically disable itself (i.e. enter banknote reject state) until the error state has been cleared.

#### Note Acceptor Disabled on High Credit Balance

9. Gaming Equipment software must incorporate a facility which will automatically disable the banknote acceptor once the credit balance of the gaming equipment or account, if appropriate exceeds [BKNTLIM] expressed in dollars.
10. This level is to be displayed to the patron in the following form or similar:  
*"Notes not accepted if Credits over \$x are registered"*.

#### Access

11. The software must be able to detect access to the following doors or secure areas:
  - (a) external door(s);
  - (b) cash box door(s);
  - (c) logic area door(s); and

- (d) banknote acceptor doors.
- 12. Access to banknote acceptor components and banknote storage areas is to be secured via separate key locks. Both are to be fitted with 'door open/close' sensors.
- 13. The gaming equipment shall be designed so that when installed according to the manufacturer's instructions, power and data cables are not accessible to the general public.

### 3.3 Physical Integrity

#### Simultaneous Inputs

- 1. The program must not be adversely affected by the simultaneous or sequential activation of various inputs.

#### External Mechanism Affecting Play

- 2. There shall be no external mechanism (DIP-switches, jumpers, etc.) that can affect the outcome of a play.

### 3.4 Interference

#### Power Supply

- 1. Gaming Equipment and associated equipment within the Gaming Equipment shall comply with relevant and applicable EMI, EMC and safety standards.

### 3.5 Information Display

#### Video Monitors

- 1. Where adjustment mechanisms for a video display unit are provided for use by gaming attendants (i.e. not service technicians), they shall:
  - (a) be clearly labelled;
  - (b) not require the use of a tool of any kind; and
  - (c) be accompanied by detailed instructions in the Operator's Manual.

#### Printers

- 2. If a gaming equipment is equipped with a printer, it must be located in a locked area of the gaming equipment (e.g. require opening of the main door) but not in the logic area or the cash box.

### 3.6 Cash Input Systems

#### Programmable Coin Validators

- 1. In the case of coin validators which are electronically programmable to recognise a coin, the coin validator must be pre-programmed at the factory and it must not be capable of being reprogrammed in the field without access to the equipment used at the factory (or without detailed technical knowledge).

#### Program Resumption Procedures

- 2. On program resumption, the following procedures must be performed as a minimum requirement:
  - (a) communications to an external device must not begin until the program resumption routine is completed successfully;
  - (b) all control programs and critical memory must be checked for corruption.
- 3. The software must be able to detect any change in the gaming equipment program from when the gaming equipment was last powered down or interrupted. If a change has been detected, the gaming equipment must lock-up, displaying an appropriate message until the lock up is cleared.

### 3.7 Events and Conditions

#### Audible Alarm

1. A technique should be provided to enable authorised personnel to adjust the volume level (without the need to enter the logic area). However, the adjustment of the volume shall not allow the alarm output to be below a threshold level whereby the alarm cannot be heard with the door shut in a typical gaming environment (volume controls secured in a logic area are exempted).

#### Action on Occurrence of a Condition or Fault Event

2. Events listed in *Table 1: Gaming Equipment Faults and Remedial Actions (If Applicable)* and *Table 2: Gaming Equipment Door Open/Close Definitions* must cause a clearly displayed message that an event has occurred and, unless otherwise indicated, must also result in the following:
  - (a) all player inputs must be disabled except for a Service Button and, optionally, any inputs required for Audit Mode. This includes disabling credit input;
  - (b) an identifiable alarm must be sounded for at least 1.5 seconds;
  - (c) game play must be saved in its current incomplete condition. The game must be paused immediately;
  - (d) cash out of any kind is to be disabled (if the gaming equipment was in a hopper payout, the hopper must be turned off and the brake applied) However, cash out may occur on a banknote jam; and
  - (e) credit input must be disabled (may be re-enabled for the duration of a credit input test or hopper test).

#### Action on Clearance of a Condition or Fault Event

3. The following actions must be performed upon clearing of a condition or fault event:
  - (a) the relevant condition or fault event messages must be removed;
  - (b) any relevant player inputs must be re-enabled;
  - (c) the alarm must be turned off;
  - (d) any game play when the fault event occurred must recommence from the beginning of the play or from the point at which the interruption occurred and conclude normally, using the data that was saved previously; and
  - (e) if the condition was a door open, a message is to be displayed stating that the door(s) has been closed until the next game play.

#### Faults to be Treated as Events

4. The following table defines faults that are to be treated as events, together with the remedial action to be taken to clear the event:

**Table 1: Gaming Equipment Faults and Remedial Actions (If Applicable)**

Fault:	Definition:	Cleared by:
<b>Coin Yo-Yo</b>	Inserted coin detected moving in the incorrect direction: A single Coin Yo-Yo may be treated as an information only event Consecutive Coin Yo-Yos are to lead to a gaming equipment fault condition	Cleared by an attendant intervention, e.g. key activation
<b>Coin-in Jam</b>	Coin detected not moving - e.g. sensors are continually blocked	Cleared by an attendant intervention, e.g. door open/closed
<b>Coin to Cashbox or Diverter Fault</b>	Coins (exceeding a manufacturer-defined amount or ratio) detected going to the cashbox instead of the hopper, or vice-versa. (count of misdirected coins may be reset on power-up)	Cleared by the fault being rectified.

<b>Excessive Meter Increment</b>	A master meter has increased by more than the increment threshold since the end of the previous play.	Cleared by attendant intervention, e.g. key activation
<b>Hopper Empty</b>	Coins not passing a hopper output sensor within a specified time	Cleared by an attendant intervention, e.g. door open/closed
<b>Hopper Jam</b>	The hopper output sensor(s) are blocked	Cleared by an attendant intervention, e.g. door open/closed
<b>Extra Coin Paid</b>	Single coin passed hopper sensor after hopper payout completed	Cleared by an attendant intervention, e.g. door open/closed
<b>Hopper Run-away</b>	Multiple coins passing hopper sensor	Cleared by an attendant intervention, e.g. door open/closed
<b>Hopper Failure</b>	Disconnection or failure of the hopper (not covered by other fault definitions)	Cleared by an attendant intervention, e.g. door open/closed
<b>Reel Not Spinning Freely</b>	Software detecting a reel not spinning correctly	Cleared by an attendant intervention, e.g. door open/closed
<b>Illegal Reel Movement</b>	Software detects unauthorised reel movement	Cleared by an attendant intervention, e.g. door open/closed
<b>External Peripheral Controller Fault /Disconnect</b>	Any Peripheral controller fault or communications failure (e.g. a Progressive Display Controller)	Cleared by technician
<b>Printer Paper Low (if applicable and possible)</b>	The printer paper will soon be exhausted. This should lock up the gaming equipment upon completion of a predetermined number of tickets calculated to ensure "Paper Out" is not possible. If a paper out sensor is also provided then "Paper Low" results only in a message. Note that if a gaming equipment has a printer it must have a paper low or paper out sensor or both.	Paper low condition to be cleared by replacement of paper (paper low signal removed) or positive attendant intervention, e.g. key activation
<b>Printer Paper Out</b>	The printer paper has been exhausted. The gaming equipment must lock-up until the paper out state is cleared	Paper out condition to be cleared by replacement of paper (paper out signal removed) and positive attendant intervention, e.g. door open/closed
<b>Printer Jammed</b>	The printer paper is not feeding correctly	Paper jam condition to be cleared by clearance of jam (paper jam signal removed) and positive attendant intervention, e.g. door open/closed
<b>Printer Failure</b>	Software detects that the printer has not been able to correctly print a ticket	Cleared by technician
<b>Printer Disconnected</b>	Software detects that the printer has been disconnected	Cleared by technician
<b>Mechanical Meter Disconnected</b>	Software detects that the mechanical meters have been disconnected	Cleared by technician



<b>Low RAM Back-up Battery</b>	Back-up RAM Battery has reached a voltage where back-up will become unreliable soon: A message stating that the repairer must be called urgently must be displayed The gaming equipment must lock-up until the battery low event is no longer present and positive indication has been given by an attendant, e.g. jackpot reset key engaged	Cleared by technician
<b>Critical RAM Errors, Mismatch</b>	Some critical RAM error has occurred: When a non-correctable RAM error has occurred, the data on the gaming equipment can no longer be considered reliable. Accordingly, any communication to external devices must cease immediately An appropriate message must be displayed Access to electronic meters must still be available	Full RAM clear by Technician
<b>Low Memory</b>	The gaming equipment has detected that it is running low on memory and cannot continue operation. Detection of this fault must occur before a total 'out of memory' condition corrupts RAM or crashes the gaming equipment. This fault may be considered a recoverable RAM error if it occurs for volatile memory, otherwise it must be deemed an irrecoverable RAM error. This fault is applicable only to gaming equipment which use dynamically allocated RAM.	Cleared by Technician if recovery possible with no loss of Critical Memory, else full RAM clear by Technician must occur.
<b>PSD Error</b>	The software has failed its own internal security check. Any communication to external devices must cease immediately. An appropriate message must be displayed, if possible. No modifications to critical meters in RAM must be possible. The gaming equipment must lock-up until the fault is rectified.	Full RAM clear or replacement of PSD by a technician.
<b>Banknote acceptors</b>	Banknote access or storage area door opened/closed	Cleared by attendant
	Banknote receptacle removed/replaced, if the banknote storage area uses a receptacle	Cleared by attendant
	Banknote jams	Cleared by attendant
	Banknote YoYo, if a YoYo is physically possible	Cleared by attendant
	Excessive banknote rejects (indicating that perhaps an attack is happening on the gaming equipment). Excessive is defined to be ten (10) consecutive	Cleared by attendant

	rejects. (count may be reset on power-up)	
	Banknote acceptor cable disconnected	Cleared by technician
	Banknote acceptor receptacle full	Cleared by attendant

5. The following table defines Door Open/Close events:

**Table 2: Gaming Equipment Door Open/Close Definitions (If Applicable)**

Event:	Definition:
<b>Gaming Equipment Door Open</b>	The main cabinet door (as defined by the manufacturer) has opened
<b>Cash box Door Open</b>	The cash box door has opened
<b>Logic Area Door Open</b>	The main CPU door has opened. This event is to cause the gaming equipment to lock up until the door is closed and the event cleared by an approved method, e.g. command from a host computer system
<b>Banknote acceptor door open</b>	The banknote acceptor door has been opened
<b>Banknote stacker door open</b>	The banknote acceptor stacker door has been opened
<b>Other external door open</b>	Any other secure area has been accessed (e.g. belly door, top box door, etc.)
<b>Gaming Equipment Door Closed</b>	The main cabinet door (as defined by the manufacturer) has closed
<b>Cash box Door Closed</b>	The cash box door has closed
<b>Banknote acceptor door closed</b>	The banknote acceptor door has been closed
<b>Banknote stacker door closed</b>	The banknote acceptor stacker door has been closed
<b>Logic area Door Closed</b>	The main CPU door has closed
<b>Other external door open</b>	Previously accessed secure area has been secured

**Non-fault Gaming Equipment Events (If Applicable)**

6. The following table lists the non-fault gaming equipment events that must be reported to the user and the respective procedures must be performed:

**Table 3: Non-fault Gaming Equipment Events**

Fault:	Definition:	Cleared by:
<b>Gaming Equipment Power Off</b>	<p>The gaming equipment has been powered off:</p> <p>(a) any game play must be saved in its current incomplete condition (reels may finish spinning, but any wins must only be paid on clearing of the error);</p> <p>(b) if the gaming equipment was in hopper payout, the hopper must be turned off and the brake applied; and</p> <p>(c) all requirements from gaming equipment faults (sections to inclusive) must be adhered to.</p>	Cleared by: gaming equipment Power On

<b>Gaming Equipment Power On</b>	The gaming equipment has been powered on: (a) any relevant player inputs must be re-enabled; and (b) any game play when the event occurred must recommence from the beginning of the play or from the point at which interruption occurred and conclude normally, using the data that was saved previously.	See definition
<b>Standalone Progressive Award</b>	A Standalone progressive prize has been won: (a) an appropriate message must be displayed; and (b) unless the prize is transferred to the player's credit meter the software must lock-up until the award has been paid by the attendant	See definition
<b>Linked Progressive Award</b>	A linked progressive prize has been won: (a) an appropriate message must be displayed; and (b) unless the prize is transferred to the player's credit meter or paid through an automatic printing of prize ticket the software must lock-up until the award has been paid by the attendant.	See definition
<b>Substantial Win</b>	Any prize equalling or exceeding the Substantial Win Amount [LARGEWIN - \$10,000] in a completed game, shall instigate this event.	Cleared by an attendant.
<b>Maximum Hopper Pay out Exceeded</b>	A cash out attempts which exceeds the Maximum Hopper Payout amount [MAXHOPPER] shall require the gaming equipment to perform a cancel credit manual pay for the full amount (or a ticket printout in accordance with the relevant sections of this document). MAXHOPPER is entered via Setup Mode or CMS parameter.	Cleared by: Cancel credit confirmation by attendant, completion of ticket print out or the player cancelling the cash out.

### 3.8 Notification of Faults

1. To assist with service and fault diagnosis, the nature and location of any fault must be displayed by a message in English (if possible this message is not to be abbreviated).

### 3.9 Data Retention

1. Non-volatile memory must be capable of reliably preserving its memory contents for at least 90 days with the mains power switched off.
2. Non-volatile memory must be checked for integrity at least every 24 hours where possible and applicable.

### 3.10 Hashing Algorithm

1. The hashing algorithm for the verification of gaming equipment software, firmware and PSDs is the HMAC-SHA1 or better algorithm. References to the calculation of hashing algorithm signatures require the use of the HMAC-SHA1 or better algorithm unless otherwise stated.

### 3.11 Critical Memory

1. Critical memory storage shall be maintained by a methodology that enables errors to be identified

#### Contents of Critical Memory

2. Critical memory which must be stored in non-volatile memory is to store all data that is considered vital to the continued operation of the gaming equipment. This includes, but is not limited to:
  - (a) all auditing meters;
  - (b) current credits;
  - (c) gaming equipment game configuration data;
  - (d) information pertaining to the last two plays (including the current play if incomplete);
  - (e) software state (the last normal state the gaming equipment software was in before interruption);
  - (f) RNG seed(s), and
  - (g) information pertaining to the last two tickets printed
3. To cater for disruptions occurring during the update process of Critical Memory, at any point in time during an update there must exist sufficient information that will allow the software to fully cater for such disruptions.

#### Detection of Corrupted Memory

4. A validity check of the entire contents of gaming equipment Critical Memory must be undertaken at least after every restart of the equipment, transaction of significance (e.g. banknote input, logic door closed, large win, jackpot win, door closed, parameter change or reconfiguration) and at the beginning of a game play (finishing before the result of the game is determined) and after a game play. After a gaming equipment restart (e.g. power off and on), the gaming equipment must complete its validity check of the Critical Memory area.
5. Any failure of a validity check is to be considered either a:
  - (a) Recoverable Memory Corruption (optional) if at least one copy of Critical Memory is established to be good, or
  - (b) Unrecoverable Memory Corruption.

#### Critical Memory Requirements

6. A proven, robust and reliable mechanism shall be implemented to check for any corruption of critical memory locations.

#### Unrecoverable Critical Memory

7. An unrecoverable memory corruption must result in a memory error.
8. The RAM must not be cleared automatically and must require a full RAM clear.

#### Non- critical RAM

9. All other RAM must be checked for corruption at each power up.

**Program Execution**

10. The gaming equipment must prevent or detect unexpected or malicious changes to program code that provides functionality central to the operation of the gaming equipment or game.
11. If unexpected or malicious changes are detected the gaming equipment must enter an unrecoverable RAM error (requiring a full RAM clear) and display an appropriate error message.
12. Where the gaming equipment expects changes to program code, the manufacturer must submit details of the expected changes to the gaming equipment tester.

**Communication Error Detection**

13. Where critical data and information (e.g., credits, metering information, information pertaining to a game outcome, etc.), is transferred between microcontrollers, there must be error checking on the transferral. This check must be at least a Cyclic Redundancy Check (CRC). Parity checking or simple check sums are not adequate.

**3.12 PSD Integrity**

1. The entire contents of all PSDs in the executable address space of a critical processor must be validated when:
  - (a) the CPU is reset;
  - (b) initiated via Audit Mode; or
  - (c) initiated by a monitoring system that requires software signature results.

**Unused Program Memory Storage**

2. The integrity of the operation of the device must be protected from nefarious or accidental use of the unused portions of the program memory storage media.

**3.13 RAM Clear**

1. There must be no method providing a 'RAM clear' to clear the meters and other areas of electronically stored data without first accessing the logic area of the gaming equipment or other secure method.
2. All memory locations intended to be cleared as per the NV memory clear process shall be fully reset in all cases. For games that allow for partial RAM clears, the methodology in doing so must be accurate.
3. The default reel position or game display after a RAM reset must not be a winning combination on any selectable line. The default game display upon entering game play mode must also be a non-winning game.
4. A configuration setting that is required to be entered during Setup Mode immediately following a RAM Reset must not be able to be changed after the equipment leaves Setup Mode.

**3.14 PSD Security**

1. PSDs must be protected from unauthorised modification.
2. Any unauthorised modification of the contents of a PSD should be logged as an event.

**3.15 Meters and Data**

1. Whenever credits are staked then the number of credits staked shall be immediately subtracted from the player's credit meter.
2. It is permissible to update the credit meter before the completion of play provided that:
  - (a) critical memory is updated when the credit meter is updated; and
  - (b) it is not possible to wager any credits transferred to the credit meter on gamble.

**Binary Meters**

3. If the metered value exceeds the highest number, e.g.  $2^{32} - 1$ , the appropriate meter is to automatically 'roll over' to 0.

**Credit Meter Prize Update and Progressive Prizes**

4. The meter must roll over to zero upon the next occurrence, any time the meter exceeds ten (10) digits and after 9,999,999,999 has been reached or any other value that is logical.

**3.16 Self-Audit Error Checking****Self-Audit Check Formula**

1. A gaming equipment shall perform a "self-audit" of the appropriate master accounting data meters as described in the following formula:

$$\text{Credit Balance} = [(\text{Coins IN} + \text{Banknotes IN} + \text{Ticket IN} + \text{Cashless IN} + \text{Total WINS}) - (\text{Coins OUT} + \text{Cancel Credits} + \text{Cashless OUT} + \text{Ticket OUT} + \text{Turnover})]$$

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

**Occurrence of Self Audit Check**

2. The self-audit check shall be performed at least at the following times:
  - (a) At the start of every play.
  - (b) Before commencing any process that transfers any monetary value out of the gaming device (e.g. hopper pay, cancel credit/ticket pay or credit transfer out).

**Action on Failure of Self Audit Check**

3. The gaming equipment shall enter an Unrecoverable Memory Corruption state in the event that this self-audit check fails.

**Meter Increment Test**

4. At the end of each play, the value of the following master meters must be compared to value of the same master meter at the end of the previous play:

Master Meter	Increment Threshold
COINS IN	\$1,000
BANKNOTES IN	\$10,000

5. If the change in the value of the master meter is greater than or equal to the increment threshold, the gaming equipment must register a fault event and display the error message 'Excessive Meter Increment' (Gaming Equipment Faults).

**3.17 Test or Diagnostic Mode**

1. No meters (other than a temporary on-screen credit meter) shall be affected by any test mode.
2. All test modes must be clearly indicated.
3. Test/Diagnostic Mode may be entered via an appropriate instruction from an attendant during an Audit Mode access.
4. Opening the main cabinet door of the gaming equipment shall not provide automatic entry to Test/Diagnostic Mode.
5. If the gaming equipment is in a game test mode, the device shall clearly indicate that it is in a test mode, not normal play.
6. If there are any test-mode states which cannot be automatically exited, then the action necessary must be indicated on the device and in the relevant manuals.

**Hopper Test**

7. If a Hopper test is implemented, the following requirements must be met:
  - (a) the main door of the device must be opened immediately prior to the hopper test commencing;
  - (b) only a specific number of coins are dispensed at each test;

- (c) a play cannot commence/continue until all coins dispensed are re-inserted into the hopper via the coin acceptor mechanism; and
- (d) there must be visual indication of the number of coins dispensed and re-inserted.

#### **Coin IN Validation Test**

8. If a coin in validation test is provided, the following conditions must be met:
  - (a) the number of coins accepted as valid by the comparator is displayed, and
  - (b) the number of coins passing coin direction sensors is displayed
 Note: Alternative implementations such as providing indicators of the line status (jammed, activated, faulty etc.) of the validator outputs and diverter outputs are acceptable if at least the same level of diagnostics is achieved.

### **3.18 Configuration**

#### **Validation of Gaming Equipment Configuration Settings**

1. All configuration settings required for the proper operation of the gaming equipment must be entered before the device can leave Setup Mode. If all configuration settings required have not been entered, the device must detect this condition and remain in Setup Mode.

### **3.19 Audit Mode**

1. Audit Mode is to include, as a minimum the following requirements:
  - (a) display of all electronic meter information;
  - (b) Last Play Recall;
  - (c) display of terminal identification;
  - (d) display of software/game identification;
  - (e) display of game configuration; and
  - (f) on-screen hashing algorithm signature results.
2. The gaming equipment's audit functionality must provide for:
  - (a) the input and display of a signature key;
  - (b) the on-screen display of an identifier for each PSD;
  - (c) the on-screen display of the HMAC-SHA1 signature for each PSD for the signature key entered; and
  - (d) the on-screen display of the master result.

#### **Signature Key Entry**

3. The gaming equipment must allow the manual entry of a signature key for the hashing algorithm. Signature key entry must be via an interface provided by the gaming equipment and there must be an on-screen legend displayed. The default signature key is hexadecimal 00.  
Signature key entry is to be: -
  - (a) in hexadecimal characters,
  - (b) of up to 40 characters in length,
  - (c) entered least significant bytes (LSB) first; and
  - (d) formatted for display with a space between every 4 characters.

#### **Master Result (for Gaming Equipment with multiple PSDs)**

4. For gaming equipment with multiple physical or logical PSDs the Master Result is a result from individual signature results of each physical/logical PSD in the gaming equipment 'exclusive-OR'ed' (XOR) together.

#### **Display of PSD Hashing Algorithm Signature Results**

5. The gaming equipment must display the PSD Descriptions, signature key and hashing algorithm signature results. The display must be able to be paused indefinitely in order to verify the displayed data. The signature key and hashing algorithm signature results must be displayed in hexadecimal characters (either all uppercase or all lowercase), and formatted with a space between every 4 characters.

Example:

Signature key: 64c5 f08e 45f1 5ad7 8031 0ccd 306a e94c c262 64e4

PSD Description HMAC-SHA1 Hex signature result

Master Result: 5aa5 c54f 8622 d7ae a78e c394 249a 3fe9 2535 465a

System PSD 1: 6651 1216 9cc0 d1df 679d 9240 38cf 8db7 1410 47e1

System PSD 2: 01c8 4a2f da32 4580 3a6a 97dc 5095 8c57 659f 83b7

Game PSD 1: 41ba 1b98 2116 31db 1b39 507d 579c 28c5 61f8 9981

Game PSD 2: 2077 335e 5834 4ef8 b68e cc65 66b1 bc89 ad37 d49d

I/O Firmware: 4c94 72e6 073f defa 7720 f873 08af de68 64c7 d546

If the results cannot be displayed on one screen, they may be displayed across multiple screens.

### 3.20 Random Number Generator and Symbol Selection

#### Game Result Determination

1. Game software must generate random symbols (or reel stop positions) from a Random Number Generator (RNG) algorithm and mapping algorithm.
2. The game software must not determine the outcome of a play (critical to the game result) or gamble until after all player options pertaining to the play or gamble have been made.

#### Fundamental RNG Requirement

3. The fundamental requirement is that the use of a RNG results in the selection of game symbols or production of game outcomes or selection of "mystery" jackpot values which are able to be proven to:
  - (a) be statistically independent;
  - (b) be uniformly distributed over their range;
  - (c) pass various recognised statistical tests; and
  - (d) be unpredictable.

RNG tests that may be applied include:

1. chi-square test;
2. equi-distribution (frequency) test;
3. gap test;
4. poker test;
5. coupon collector's test;
6. permutation test;
7. run test (Patterns of occurrences should not be recurrent);
8. spectral test;
9. serial correlation test potency and degree of serial correlation (outcomes should be independent from the previous game); and
10. test on sub sequences.

#### Choice of Algorithm

4. The choice of algorithm is at the discretion of the equipment supplier, however it must comply with the requirements of this document.

#### Background RNG Activity Requirement

5. The RNG must be cycled continuously between plays.

#### RNG Seeding

6. The method of seed-set generation must be approved.
7. The method of seed generation must ensure that:
  - (a) the same sequence of random numbers is never used in more than one device at the same time (i.e. there is to be a method whereby each gaming equipment has a unique seed generation technique or RNG start-up values).
  - (b) the "next" game outcome is not able to be predicted.
8. Seeding and re-seeding must be kept to an absolute minimum. Both the method of re-seeding and the instances when it may occur must be approved. Re-seeding should not



in general be under operator control. Re-seeding should not be a routine or regular practice.

9. If for any reason the background RNG activity is interrupted (e.g. gaming equipment power down), the next input variable(s) for the RNG must be a function of the value(s) produced by the RNG immediately prior to interruption.

#### **RNG Minimum Period**

10. The period of the RNG must be greater than its range.

#### **Minimum Range Requirement**

11. The range of values produced by the RNG must be adequate to provide sufficient precision and flexibility when setting event outcome probabilities, (i.e. so as to accurately achieve a desired expected RTP).

#### **Mapping**

12. Mapping of random numbers into symbols (or reel stop positions) should observe the following principles:
  - (a) the output resulting from the mapping of an RNG to symbols (or reel stop positions) must not be predictable;
  - (b) any outcome derived from the random number generator are uniformly distributed;
  - (c) any mappings to convert random numbers into game symbols are linear, and the distribution of the mapped symbols is identical to the distribution of the unmapped random number from which they were derived;
  - (d) the mapped random number sequence must demonstrate that they are statistically random when subject to the same statistical tests for randomness specified for the base random number generator;
  - (e) the game outcomes which are derived from either a combination of mapped symbols or directly from the unmapped random numbers must have the same distribution and probability of occurrence as the game that the device implements. In particular, poker games must have the same firsthand distribution and probability as hands dealt from a randomly shuffled deck of cards; spinning reel games must have the same outcome probabilities and outcome distribution as the physical model upon which the game is based, and so on; and
  - (f) the mapping of numbers directly from the RNG output or through a scaling algorithm shall not influence a symbol to occur with a probability not equal to its statistical expectation.

#### **Scaling Algorithms**

13. If a random number with a range shorter than that provided by the RNG is required for some purpose within the gaming equipment, the method of re-scaling, (i.e. converting the number to the lower range), is to be designed such that all numbers within the lower range are equally probable.
14. If a particular random number selected is outside the range of equal distribution of re-scaling values, it is permissible to discard that random number and select the next in sequence for the purpose of re-scaling.

### **3.21 Probability**

1. The probability for attaining any advertised prizes and events must not be less than 1/7,000,000 (at a rate of at least 1 in 7 million plays).
2. The calculation of the probabilities is to:
  - (a) be based on game play with the maximum number of possible lines, ways or patterns available in one play (using the configuration which provides the lowest number of 'maximum lines' etc. available in one play) and the minimum bet multiplier;
  - (b) combine the probabilities for the same prizes when occurring in different elements of a play (e.g. base and feature elements);

- (c) combine the probabilities for the same prizes occurring with and without substitute symbols where applicable;
- (d) exclude 'multipliers'; and
- (e) ignore all linked progressive jackpots.

### 3.22 Standard Deviation

1. Game submissions, possessing an NSD exceeding 18 can be considered suitable for approval provided a gaming equipment tester has independently certified that game configurations exceeding NSD 18 will provide the expected rate of return to within one per cent of the expected return configuration. Where these are requested the gaming equipment tester must base that certification on maximum lines/ways/patterns or equivalent (excluding link progressive prizes) for a minimum of 2.5 million plays using simulated game results.

In determining the NSD for a game, the following conventions must be applied:

- (a) Calculate standard deviation of the base game at minimum bet and single line play or equivalent. (Should the underlying game algorithm or randomising mechanism change with a change to play options selected (e.g. different virtual reels are activated upon a change to the number of lines played or certain prize categories are only available by selecting specific play options), the highest standard deviation result must be used);
- (b) Coinciding prizes are to be treated as separate prizes (e.g. a payline prize of 20 coinciding with a scatter prize of 50 are to be treated as two separate prizes of 20 and 50);
- (c) Feature game prize contribution must, as a minimum, be calculated using a set of individual feature prizes with corresponding weighted probabilities for each prize. (The calculation method must not use the mean of all feature prizes treated as a single base game prize);
- (d) For the purposes of (c) above, feature game prizes are to be calculated under conditions applicable to the feature when the base game is in the mode referred to in (a) above (i.e. using the same bet and line pattern or equivalent);
- (e) Gamble features (e.g. Double-up) are to be excluded;
- (f) Progressive prize components, both standalone and linked, are to be excluded;
- (g) All calculations must be made to a minimum accuracy of four decimal places and the NSD must be reported to a minimum accuracy of two decimal places.

### 3.23 Access Detection

1. A logic door open event must be stored for at least 14 days after the event, with and without mains power being available to the gaming equipment.

### 3.24 Master Meters

1. The following master meters (and units) must be available within a single, separately identifiable section of Audit Mode:

**Table 4: Master Meters (If Applicable)**

METER	Definition	UNITS
<b>GAMES PLAYED</b>	total number of games played	[plays]
<b>TURNOVER</b>	total value in dollars of bets made from the player's credit meter (note gamble bets such as double up are not bet from the player's credit meter)	[\$.]
<b>TOTAL WINS</b>	total value in dollars of all prizes awarded to the player's credit meter (incl. Residual Credit Gamble prizes)	[\$.]

<b>CANCELLED CREDITS</b>	total of all credits cancelled from the Credit meter by attendant and all credits paid from the Credit meter by ticket	[\$.]
<b>CASH BOX</b>	total of all coins deposited to the cash (drop) box	[\$.]
<b>COINS IN</b>	total of all coins in but not hopper refills	[\$.]
<b>COINS OUT</b>	total of all coins out from hopper, but not extra coins out or short pays	[\$.]
<b>EXTRA COIN OUT</b>	total of all coins detected as dispensed in error from hopper (excluded from “coins out”)	[count]
<b>BANKNOTES IN</b>	total of all banknotes accepted, if applicable.	[\$.]
<b>CASHLESS IN</b>	total of all credits electronically transferred to the gaming equipment (if applicable), or paid to credit meter and not added to Total Wins	[\$.]
<b>CASHLESS OUT</b>	total of all credits electronically transferred from the gaming equipment, if applicable	[\$.]
<b>MONEY IN</b>	total value in dollars of coins and or banknotes inserted to register credits on the player’s credit meter together with transfers to the gaming equipment to register credits on the player’s credit meter	[\$.]
<b>MONEY OUT</b>	total value in dollars of credits redeemed from the player’s credit meter by hopper pay, ticket print, cancelled credit or account transfer, but not extra coin out errors or short pays	[\$.]

Note: where a master meter is not relevant, its value may be displayed as “N/A” or null.

2. A gaming equipment which contains a banknote acceptor device must maintain sufficient metering to be able to report the following:
- total monetary value of banknotes accepted (Banknote Money In);
  - total number of banknotes accepted (Banknote Counts);
  - counts of all rejected banknotes (Banknote Rejects);
  - the number of banknotes accepted for each banknote denomination; and
  - the value of the last five banknotes accepted (with time stamps).

Note: That these matters are Master Meters, i.e. to be cleared only on Master Reset of the gaming equipment.

#### **Banknote Clearances**

3. To provide adequate information to assist in the reconciliation of actual currency cleared from a banknote acceptor, the gaming equipment must maintain the following data and report via an Audit screen and/or appropriate Banknote Clearance ticket to the Venue Operator each time a banknote clearance operation is performed:
- total monetary value of banknote expected to be removed from the banknote storage area, i.e. held in the removed receptacle; and
  - total monetary value of banknotes denomination expected to be removed from the banknote storage area.

#### **Soft Meter Update**

4. A meter must be updated on the occurrence of the event. All meters must be added to, not incremented with the exception of coin handling meters (i.e. coin in and out meters). The term “added to” indicates the fetching of the current value from memory, conducting an arithmetic add operation and storage of the accumulated value in memory.

#### **Credit Meter**

##### Credit Meter Decrement

5. Whenever credits are staked (e.g. commencement of play, additional wagers during a play) then the number of credits staked shall be immediately subtracted from the credit meter.

- Update of the Credit Meter**
6. The end of a play is defined to be when all appropriate meters for a game have been updated. It is permissible to update the credit meter before the completion of play provided that:
- critical memory is updated when the credit meter is updated; and
  - only credits held on a win meter may be wagered on a gamble feature, i.e. it is not possible to wager any credits transferred to the credit meter on a gamble feature.

**Credit Meter Prize Update and Progressive Prizes**

7. The value of every prize (at end of a play) must be added to the credit meter, except progressive prizes. Progressive prizes may be added to the credit meter if the:
- credit meter is maintained in dollars and cents; or
  - progressive meter is incremented to whole credit amounts; or
  - prize in dollars and cents is converted to credits on transfer to the credit meter in a manner that does not mislead the player (e.g. make unqualified statement “wins meter amount” and then rounds down on conversion) or cause accounting imbalances.

### 3.25 Definition of Software Meters

**Progressive Meters (If Applicable)**

1. Standalone progressive gaming equipment must display upon request the following additional meters (in order) for each progressive prize offered:

**Table 5: Progressive Meters**

METER:	Definition:	UNITS:
<b>CURRENT VALUE</b>	current prize amount	[\$.]
<b>OVERFLOW</b>	amount exceeding ceiling	[\$.]
<b>HITS</b>	number of hits for this progressive	[count]
<b>WINS</b>	total value of wins for this progressive	[\$.]
<b>STARTUP</b>	startup value	[\$.]
<b>CEILING</b>	ceiling value	[\$.]
<b>INCREMENT</b>	percentage increment rate	[%]
<b>HIDDEN INCREMENT</b>	percentage increment rate for the reserve pool	[%]
<b>INITIAL VALUE</b>	initially entered after last RAM clear. (Used for creating a ‘lost’ jackpot.)	[\$.]

**Multi-game Meters**

2. For each game in a multi-game configuration, the following must be recorded and displayed in the following order:

**Table 6: Multi-game Meters (If Applicable)**

METER:	Definition:	UNITS:
<b>GAMES PLAYED</b>	total number of games played	[plays]
<b>TURNOVER</b>	total of all bets made from the credit meter	[\$.]
<b>TOTAL WINS</b>	total of all wins, but not interim gamble wins	[\$.]

**Residual Credit Removal Meters**

3. If residual credit removal meters are provided, the following meters must be recorded and displayable in audit:

**Table 7: Residual Credit Removal Meters (If Applicable)**

<b>METER:</b>	<b>Definition:</b>	<b>UNITS:</b>
<b>RCR STROKE</b>	the number of times residual credit removal play has been used	[count]
<b>RCR TURNOVER</b>	residual credit removal turnover	[\$.]
<b>RCR WIN</b>	residual credit removal wins	[\$.]

Note: RCR meters can be a separate game, or a part of the last played game.

### 3.26 Printed Tickets

1. The gaming equipment must retain electronic records for the last thirty-five (35) tickets printed.

## 4 Gaming equipment monitoring and control

### 4.1 Configuration Requirements

1. The CMS shall provide a function for registering a new gaming machine with a unique identifier (e.g. Serial Number or Asset Number) and a unique floor location.
2. The system shall not permit duplicate creation of the unique identifying fields.
3. The CMS shall support the capability to register and report all configuration information associated with a gaming machine. As a minimum, the CMS shall support the following:
4. Unique identification number (Serial Number or Asset Number);
  - a. Unique Floor location number;
  - b. Status of the game;
  - c. Manufacturer Name;
  - d. For each game provide the following:
    1. Game Name;
    2. Denomination of the game;
    3. Jackpots configured for the game; and
    4. Theoretical hold of the game with & without jackpot contributions;
  - e. Base/Shell/OS program identifiers;
  - f. Game program version number;
  - g. Accounting meters (as specified in relevant sections of this document); and
  - h. Functionality supported such as Ticket In/Ticket Out, Cashless, etc.
5. The CMS shall be capable of reading each gaming machine configuration directly from the gaming machine by using its unique id.
6. The CMS shall be capable of reading each individual gaming machine meters directly from the gaming machine.
7. The CMS shall maintain a history of changes made to the configuration of all gaming machines for a minimum of the prior 12 months.
8. The CMS shall maintain a history of changes made to the configuration for a given floor location for a minimum of the prior 12 months.
9. The CMS shall have the capability to print and/or display all the retained historical information based on the unique identifying fields.
10. The CMS shall be capable of designating which gaming machines offer jackpots.
11. The CMS shall provide the capability to account for standalone jackpot configurations.
12. All information relating to jackpot/progressive configuration and winnings shall be maintained in the CMS.
13. The CMS shall support the capability of issuing real time commands to the gaming machine for information retrieval and gaming machine control functions.
14. The CMS shall store the history of all machine events online, near-line or offline for a minimum period of 12 months. It shall support the capability for generating alerts for illegal events and unexpected gaming data (e.g. illegal door open, illegal drop box access, high win, etc.).
15. The date and time displayed by the CMS shall be in the current local time.
16. The CMS shall provide the capability to easily attach/detach gaming machines with jackpot configurations to/from the jackpot system.

### 4.2 Game Verification

17. Game verification shall be automatically triggered for specific event(s) or initiated by a user command from the CMS or from the EGM if supported. To ensure full coverage, gaming verification should be performed after each of following incidents:
  - a. EGM power up;
  - b. Initial establishment of communication to the CMS;
  - c. Game win over a specified amount; and
  - d. Loading of the program files.

1. CMS shall generate an exception when a signature verification failure occurs on any EGM.
2. When a signature check failure is recognised, the failed EGM shall be prevented from performing any monetary transaction.

#### **4.3 Metering**

1. The CMS shall be able to collect and individually report all the meters specified in relevant sections of this document.
2. Real-time meter data retrieved from an EGM must be stored as gross values and not as an incremental or delta values.
3. Meters or files associated with player entitlement shall be securely stored and any alternation to these accounts must result in an audit trail or a log file.
4. At a minimum, the CMS shall collect and store all the meters specified in relevant sections of this document from all the gaming machines at a period as agreed by the VCGLR.
5. Meter information shall be stored and made retrievable from online, near-line or offline storage for a minimum period of five (5) years.
6. The CMS shall be capable of storing meters to at least ten digits or any other value that is logical.
7. The CMS shall store the history of all meter changes. It must not be possible to alter the history of these changes made to the meters.
8. The CMS shall store adequate meter information in order to recover the last known valid meters under situation such as machine RAM corruption.
9. The CMS shall report all instances where it receives no end-of-day meter values from a gaming machine or it has calculated a suspect meter value for a gaming machine, so that the circumstances can be investigated, and the meter values entered or altered manually.
10. The CMS shall be capable of producing reports with calculations based on absolute meter values obtained from the gaming machines within the system rather than performing calculations based on incremental values.
11. It must be possible, in conjunction with appropriate manual procedures, to calculate the correct daily revenue when the following exceptional circumstances have occurred during the day:
  - a. A RAM reset has occurred on a gaming machine;
  - b. A meter rollover has occurred on a gaming machine;
  - c. A gaming machine has been moved or retired;
  - d. A new gaming machine has been installed;
  - e. Multiple configuration changes are made for a gaming machine within one gaming day; and
  - f. A gaming machine has lost communication for a prolonged period of time.

#### **4.4 Exception Reporting**

1. The CMS shall have the capability to store and report all the events specified in relevant sections of this document.
2. Each event shall be associated with a unique number/code or description that identifies the event as well as the unique identification code for the device that is reporting the event. It will also contain a brief description of the event.
3. The CMS shall report any loss of communication to any gaming machine. In addition, the CMS shall report any loss of communication to any other critical elements if supported. It shall also report when communications are re-established.
4. The CMS shall have the capability to handle any gaming machine backwards meter movements (except credit meter), meter rollover and unreasonable meter increments.
5. The CMS shall provide a display in real time of critical events and faults that may indicate that system security or integrity is compromised.
6. At a minimum, the exception reporting facility shall have the capability to report only on selected event/s within a given period for selected devices.

7. The CMS shall have the capability to interface and forward selected events to other casino systems such as pager and surveillance systems.
8. All exception reporting shall be time stamped with the local time.
9. All exception reporting should also be stamped with the username and employee identification.

#### **4.5 Functionality**

1. The CMS shall include capability to capture and process every hand pay message from each gaming machine. A method by the CMS to provide the player/attendant with a unique transaction number for each hand pay is recommended.
2. A Hopper Fill is normally initiated from a hopper empty message. An allowable exception to hopper fill initiation would be where the system provides preventive or maintenance fill functionality, in which the transaction may be initiated by system or an authorised user.
3. Once captured, there must be access controls to allow for authorization, alteration, or void of any values prior to payment.

#### **4.6 System requirements**

##### **4.6.1 Server**

The CMS shall comprise of networked systems that direct overall operation and associated databases that stores all entered and collected information.

##### **4.6.2 Interface**

1. Each CMS interface component designed to fit within an EGM shall be installed within a secure area of the EGM and shall employ a secure communication method between the interface component and the CMS.
2. If not directly communicating EGM meters, the interface component must maintain separate electronic meters to preclude the loss of information from meter rollovers, or a means to identify multiple rollovers in the connected gaming machine.
3. If unable to communicate with the CMS, the interface component or EGM should be able to preserve all metering and exception information until at such time the information can be communicated to the CMS. If possible, EGM operation may continue until the stage that critical data will be overwritten.
4. An interface component should have a mechanism whereby an error will not cause the loss of stored accounting meter information.
5. An interface device or any other intermediate device, installed outside a secure computer room, that stores and maintains buffered/logging information containing financial information and critical event data must conform to the Critical Memory requirements specified in relevant sections of this document.
6. Data captured and stored in an interface device but not transmitted to CMS shall be preserved after a power loss to an interface component and shall be maintained for a period of at least twenty-four (24) hours.
7. Interface components shall allow for the configuration of a unique identification number, to be used in conjunction with the EGM file in the CMS.
8. The CMS shall also report and store all events reported by all the nodes other than the EGMs such as interface units, Jackpot Controllers and floor controllers etc.
9. Each event shall be associated with a unique number/code that identifies the event as well as the unique identification code for the device that is reporting the event. It will also contain a brief description of the event.



## 4.7 Security requirements

### 4.7.1 System Requirements

1. The architecture of the CMS shall be designed to provide redundancy to key critical components to limit under normal operating conditions a point of failure that could interrupt the operation of the CMS or lose any critical data.
2. The computer rooms of the central computers of the CMS shall meet the relevant sections of this document for secure computer rooms as well as the minimum infrastructure and environmental requirements of the system supplier.
3. All doors of the CMS cabinet and equipment racks shall be equipped with locks, the keys to which will be controlled by a sign-out log.
4. The computer systems shall be protected against power fluctuations and temporary loss of power by installation of a UPS or other such device.
5. The CMS shall be protected against long term loss of power by installation of a generator or other such device. The generator should have the fuel capacity to support the computer systems, air conditioning, security system, tele-communication equipment, computer terminals and sufficient lighting for normal operation of the computer room and hotline area for a period of 24 hours.
6. The central computer room must have appropriate air conditioning to maintain the environment required by the computer(s) for normal operation. There must be sufficient duplication in the air conditioning to allow the CMS to continue operation should there be a failure of a single component of the air conditioning system.
7. The computer room must have an emergency lighting system that automatically activates when mains power is lost.
8. The operating environmental systems (at least the power and air conditioning) are to be monitored by a computerised system that will perform automated switching to backup systems (e.g. mains power to generator) for most component failures of the environmental system.
9. The CMS computer room must have an appropriate automatic fire detection and protection system.
10. The CMS computer room must have appropriate measures to keep the static electricity to an absolute minimum.
11. Access to the computer room shall be controlled through physical and electronic monitoring. All access shall be recorded and logged for further verification.
12. Communications between the CMS hosts and the other gaming machines shall be protected from un-authorized access, modification or impersonation.
13. The CMS system shall incorporate a secure method to prevent modification and unauthorised viewing of all secure data associated with all critical and sensitive information.
14. The CMS shall be designed such that the access privileges required to perform different types of user functions shall be associated with different types of user accounts in order to restrict access to secure and sensitive sections of the CMS.
15. CMS hosts shall not be equipped with unsecure wireless interfaces.
16. All successful and unsuccessful (exceeding maximum attempts) access attempts to CMS hosts shall be recorded in an audit trail or a log file.
17. All passwords in the system shall be stored in an encrypted, non-reversible form.
18. The CMS shall not permit alteration of any metering data, validation data (TITO) or any other critical data and event log information that was properly communicated from the EGM.
19. The CMS may permit alteration of any metering data, validation data (TITO) and event log information that was not properly communicated from the EGM with the alteration recorded in an audit trail.
20. In the event financial data is changed, an audit log must provide at a minimum the following:
  - a. Data element & value before change;
  - b. Data element & value after change;
  - c. Time and date of change; and

- d. User(id) which performs the change.
- 1. The system(s) used for developing or testing shall be completely separated from the live system and its database.
- 2. Firewalls and/or any other industry acceptable methods must be utilised to protect against unauthorised access.
- 3. Firewalls used to protect production server networks shall be able to log audit information in a manner to secure the information from potential intrusion. The Casino Operator must document the firewall rules for VCGLR approval.
- 4. A program must be available that will list all registered users on the system including their privilege level.
- 5. CMS items (e.g. servers, gateways, communication controllers etc.) located in any area not restricted to authorised personnel shall be securely housed and physically locked.

## 4.7.2 CMS Recovery

### 4.7.2.1 Host CMS Recovery

The Licensee must have policies, procedures and standards in place in accordance with for CMS Data and software recovery. The disaster recovery site should meet the standards required for the primary site as set out in this document.

### 4.7.2.2 Transaction Logging

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

For transaction logging it is required that:

1. The CMS must record in a log file or databases (including time stamp and date stamp) critical transactions received from gaming machines, gaming equipment, jackpot systems, electronic table game systems, cashier stations, control stations, cash counters (if within the baseline) and other integral components of the CMS.
  - a. The log file(s) and/or database must be duplicated for reliability using secure storage methodology; and
  - b. All adjustments or modifications to the transactions must be recorded with the CMS operator's user ID (and time/date-stamp).
2. All transactions and events are to be written to the log in the order that they occur.
3. 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 without the appropriate System Administrator user permissions in accordance with the approved Internal Control Statement (ICS). The use of such System Administrator privileged accounts is in accordance with supervised access controls.

### 4.7.2.3 Format of Log Records

1. All log records must have a standard format with the following minimum information to be included with each log record:
  - a. The date that the transaction/event occurred;
  - b. The time that the transaction/event occurred;
  - c. The identifier for the part of the CMS for which the transaction/event occurred where supported;
  - d. Any relevant data that is associated with the event; and
  - e. A unique event identifier or description which defines the transaction/event.
2. A list and description of all transaction/event id's must be provided to the Commission and must be kept up to date by the Licensee as modifications are made to the system.

#### 4.7.2.4 Disaster Recovery and Business Continuity

1. The Licensee must have disaster recovery and business continuity capability, demonstrated through adequate backup and recovery mechanisms (including total capacity to cope with peak load, fault tolerance, security and control).
2. The Licensee must establish and maintain policies, procedures and standards for business continuity and disaster recovery.
3. The Licensee must establish and maintain a business continuity plan, and a disaster recovery plan.
4. The Licensee must establish and maintain a disaster recovery test plan, including a schedule for testing and conduct disaster recovery testing in accordance with the plan.
5. In the event of a disaster, there must be a method of ensuring where possible that all data and transactions and information related to the CMS can be rebuilt up to the point of the disaster.
6. 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.

#### 4.7.2.5 Central Site Failure Modes and Recovery

1. Following any failure, it must be possible to restore the state of the CMS and its database(s) without losing any information where possible.
2. All backup or stand-by systems should be tested regularly to ensure the timely support of the systems.

#### 4.7.3 Time Synchronization

1. The CMS shall maintain an internal clock that accurately reflects the current time (in hours, minutes and seconds) and date that shall be used to provide for the following:
  - a. Time stamping of significant events;
  - b. Reference clock for reporting; and
  - c. Time stamping of configuration changes.
2. The CMS shall support the capability of maintaining and synchronizing the time for all connected devices including EGMs within an accuracy of sixty (60) seconds to ensure that time stamping of all events and data is correct.
3. The CMS shall support capability to synchronizing time with an external reference clock.

#### 4.7.4 Duplication

The CMS shall be duplicated so that if a computer or part of a computer fails, gaming operations can continue.

#### 4.7.5 Development System

The Casino Operator must provide a fully configured development system to enable new versions of CMS software and/or hardware and new EGMs and their games to be adequately tested in an appropriate environment.

#### 4.7.6 Data Retention

1. Game play statistics, machine events, configuration data, jackpot and bonus payments data are to be held for each individual EGM in the CMS.
2. The calculated player return statistics for each game shall be maintained by the CMS.
3. Accounting and security event data are to be held for each individual EGM.
4. All payments for jackpots, bonuses and promotions information shall be maintained by the CMS.

#### 4.7.7 Code Download Requirements

1. Downloads or uploads of code from or to CMS hosts shall be secure using industry best practices.
2. An audit log shall record the time and date of any download if supported. The audit log shall also contain which version(s) of code was downloaded and who was logged in at the time of the download. In addition, appropriate system change management processes must be followed.

#### 4.7.8 System Integrity

1. The CMS system shall have the capability to authenticate the identity of all the devices included in the baseline that are connected to the CMS. This authentication shall be performed at least after each of the following events:
  - a. Initial establishment of communication to the CMS;
  - b. When initiated by an authorised user; and
  - c. Loading of program files.
2. The CMS shall be designed and developed to provide assurance of data accuracy and integrity. There shall be:
  - a. Input data validation controls to ensure that input data is appropriate;
  - b. Processing controls to detect errors in the completeness and accuracy of the processing and update of the system; and
  - c. Output data controls to ensure the accuracy of information being output or reported.
3. The integrity of the CMS software shall be maintained during operation.
4. The CMS shall have a capability to validate the identity of the device from which any communication data has originated and reject data packets received from any nodes not authenticated by the CMS.
5. The CMS shall have the capability to detect and discard any unreasonable or corrupt data information received.
6. The CMS shall have the capability to periodically authenticate the compatible baseline nodes within the system.
7. The CMS shall have the capability to manually verify the authenticity of a given compatible baseline node at any time.
8. The CMS may provide support for concurrent validation of different versions of software for the same device.
9. When a signature check failure is detected, the CMS should exclude the gaming machine/s as well as any other system components that failed the signature checking from performing any monetary transactions.

#### 4.7.9 Events

1. The CMS shall provide an online search facility that enables comprehensive searching of the event log for the present and for a minimum of the previous thirty (30) days of data or to the maximum available online storage capacity. The search facility shall have the ability to perform a search based at least on the following:
  - a. Date and Time range;
  - b. Unique interface element/EGM identification number; and
  - c. Event number/identifier.
2. Each event shall be stored in a database(s) which includes at least the following:
  - a. Date and time when the event occurred;
  - b. Identity of the EGM/node that generated the event;
  - c. A unique number that defines the event; and
  - d. A brief text that describes the event.
3. In the event of an unauthorised access of the logic area containing software, the CMS shall have the capability to raise a real-time priority exception.
4. The CMS shall generate alerts for link down detection of any EGM with minimal delay.

5. Such error conditions shall be rectified within the time frame stipulated by the Casino Operator's Internal Control Procedure with no loss of data residing on the EGM (which shall be gathered by CMS upon resumption of connectivity or EGM coming back online).

#### 4.7.10 Communications

1. The communication path between gaming machines and CMS shall be implemented using a proven and reliable communication protocol and network architecture that is robust against potential attacks.
2. Individual network segments shall be isolated from each other and protected using firewalls that are able to log audit information to a central logging host.
3. The communication protocol between the EGMs (interface cards) and CMS shall provide the following:
  - a. Error Control;
  - b. Flow Control; and
  - c. Link Control (remote connection).
4. In event an EGM is offline or the EGM has a complete loss of communication with the CMS, the EGM shall not process any financial transactions such as Voucher In/Out, Cashless In/Out etc.
5. All critical data that traverse through communications lines shall have suitable encryption or other cryptographic security methods to protect the integrity of the data. This does not apply to communications within a single logic area or communications within the secure computer room.

#### 4.8 Reporting Requirements

1. The CMS shall have the capability to generate financial reconciliation and variance reports.
2. The CMS shall provide the capability to calculate the revenue based on the soft meters collected from the gaming machines and based on the actual drop/count figures.
3. The CMS shall be able to produce a report showing the net win, theoretical win (based on gaming machine's theoretical RTP) and variances for all gaming machines.
4. The CMS shall have the capability to produce a jackpot reconciliation report that compares the jackpot contribution reported by the jackpot controller against the values calculated by the CMS from the meters reported by the EGM and reports any variances.
5. While calculating the reporting data, the values must not be rounded or truncated during the calculation in-order to eliminate any reporting errors.
6. The CMS may perform validity checks on the parameter ranges input from the user. An option to show valid parameter ranges for any user input field is recommended.
7. All reports shall support the maximum field range. Where the report is insufficient to display the information, a separate means to access this data must be provided.
8. An empty report (i.e. a valid report with no data) must conform to the same identification requirements.
9. Reporting of data for a given field shall be consistent across all the reports. Additionally, the representation of fields shall comply with local representation of similar standard fields such as currency, date and time.
10. The system shall be designed such that generation of any reports will not significantly affect the CMS response time to the gaming machines.
11. All reports are to be generated with respect to the local time zone.
12. The system shall have a capability to generate "Flash Revenue Reports" as soon as the end-of-day time is elapsed. A capability to generate an "Adjustment Report" providing details of the accounting adjustments and the final reports is also required.
13. The CMS shall include the operating username and/or employee identification or similar identifier in the reports. For systems that do not provide this capability, the Casino Operator should maintain controls to ensure all reports include the operating username or similar identifier.

## 4.9 Voucher In/Voucher Out

### 4.9.1 General

A ticket/voucher validation system may be entirely integrated into a CMS or exist as an entirely separate entity. A gaming machine or ETG supporting ticket/voucher validation capability shall be equipped with a voucher reader and a voucher printer, each of which has a communication connection to the validation system. The vouchers can either be redeemed for cash at the cage or at the Cash Redemption Terminal (CRT) or inserted for play into other gaming machines or ETG's (redeemed as credits).

Ticket/Voucher validation systems are generally classified into two types:

1. 'Voucher In & Voucher Out' systems that allows a player to insert the ticket/voucher in a gaming machine to redeem for credits and enable a player to redeem their current credits to a voucher; or
2. 'Voucher Out' systems that only allows a player to redeem their credits to a voucher.

This section primarily provides specifications for 'Voucher In & Voucher Out' system.

### 4.9.2 Voucher Types Supported

The Voucher In & Voucher Out system will support printing of a ticket for the current cashable credits when the player opts to collect them. Additionally, the Voucher In & Voucher Out systems may support either printing only or printing & redeeming for the following type of vouchers:

1. Cashable promotional credits;
2. Non-Cashable promotional credits;
3. Non-Cash bonus prizes;
4. Cancel Credit (hand Pay) tickets by an authorised Casino Operator staff; and
5. Jackpot hand pay tickets by an authorised Casino Operator staff.

### 4.9.3 Ticket/Voucher Redemption

1. Ticket/Voucher redemption on a gaming machine or any other devices such as CRT shall only be possible when the gaming device is linked to an approved validation system.
2. Validation approval shall only be originating from the Ticket/voucher validation system.
3. The validation system shall process Ticket/voucher redemptions correctly according to the secure communication protocol implemented.
4. The Ticket/Voucher host shall have the capability to validate and accept only authorised vouchers. This validation technique shall have as a minimum, the capability to prevent validation of incomplete or voided vouchers.
5. A gaming machine, ETG or CRT connected to the Ticket/Voucher system shall provide the capability for the display of relevant informative messages whenever a player-initiated Ticket/Voucher is being processed for payment.
6. The Ticket/Voucher system shall have the capability to limit accepting of tickets up to a configurable value.
7. The validation system shall update the Ticket/Voucher status on the database during each phase of the redemption process. As a minimum, whenever the voucher status changes, the following information shall be recorded:
  - a) Date and time of status change;
  - b) Ticket/Voucher status;
  - c) Ticket/Voucher value; and
  - d) Machine location or source identification from where the Ticket/Voucher information came from.
8. The validation system shall be able to identify and notify the cashier of the following conditions:
  - a. Ticket/Voucher cannot be found on file (stale date, forgery, etc.);
  - b. Ticket/Voucher has already been paid;
  - c. Amount displayed on voucher differs from the amount stored on the system (if supported); or
  - d. The Ticket/Voucher is in an intermediate/lockup state.

9. All validation terminals for cashier/change booth operation shall be user and password controlled.

#### 4.9.4 Ticket/Voucher Issuance

1. The Ticket/Voucher system shall guarantee the authenticity of any voucher generated by the system.
2. A gaming machine, ETG or CRT connected to the Ticket/Voucher system shall provide the capability for the display of relevant informative messages whenever a player-initiated Ticket/Voucher issuance is being processed.
3. Validation number to be printed on a Ticket/Voucher will be generated by the validation system.
4. The algorithm or method used by the validation system to generate the Ticket/Voucher validation number shall guarantee uniqueness and non-repetition.
5. The validation system shall only accept one (1) authorised Ticket/Voucher per valid validation number.
6. The Ticket/Voucher system shall have the capability to limit printing of tickets.
7. The validation system shall record the Ticket/Voucher information correctly and store the Ticket/Voucher information into the database.
8. The Ticket/Voucher system shall record all the details associated with Tickets/Vouchers generated by any gaming machines or gaming devices. Recommended fields to be included in a Ticket/Voucher are given below:
  - a. Casino/Establishment name;
  - b. Gaming machine unique floor location;
  - c. Date & time of voucher issuance in local time;
  - d. Amount in numeric format as well as in words;
  - e. Sequence number;
  - f. Validation number;
  - g. Type of voucher being generated (cancel credit, jackpot payment, promotional Ticket/Voucher etc.); and
  - h. Expiration period or date when the voucher will expire.
9. At any given time, the Ticket/Voucher system shall be able to identify the status of a Ticket/Voucher (e.g.: Pending, Void, Paid, Un-paid, Locked).
10. In the event communications between the Ticket/Voucher system and a gaming device is lost, the Ticket/Voucher system shall allow no more than one Ticket/Voucher that is being processed to be printed.
11. The Ticket/Voucher shall be printed on secure stock.
12. Any capability to generate offline ticket/voucher printing (if supported) shall be approved by VCGLR.

#### 4.9.5 Ticket/Voucher System Requirements

1. The Ticket/Voucher system shall be designed such that the access privileges required to perform different types of user functions shall be associated with different types of user accounts to restrict access to secure and sensitive sections of the Ticket/Voucher system.
2. The Ticket/Voucher database shall be designed such that all the critical information generated such as validation number, amount, status of the Ticket/Voucher etc. shall be stored such that it is not possible to alter this information once it is stored in the database.
3. In the event any financial data is changed, an audit log shall be generated to capture the following (at a minimum):
  - a. Validation number of the voucher;
  - b. Data element and value before change;
  - c. Data element and value after change;
  - d. Time and date of change; and
  - e. User (id) that performed the change.

4. The Ticket/Voucher system database shall be designed such that no single point failure of any portion of the system would cause the loss or corruption of data.
5. The Ticket/Voucher system shall have a capability to set an automatic validity period for Tickets/Vouchers issued by a gaming machine. Ticket/Voucher will not be accepted by the gaming machine beyond this period.
6. The Ticket/Voucher system shall be designed to ensure that a power loss or a restart of any node will not result in the loss of any Ticket/Voucher information or in the generation of duplicate Tickets/Vouchers.
7. The Ticket/Voucher system shall have the capability to generate daily monitoring logs of user accesses.
8. The Ticket/Voucher system shall have the capability to generate a report on all redeemed Tickets/Vouchers.
9. The Ticket/Voucher system shall have the capability to generate a report of all printed Tickets/Vouchers.
10. The Ticket/Voucher system shall have the capability to generate a report of all expired Tickets/Vouchers.
11. The Ticket/Voucher system shall have the capability to generate a Ticket/Voucher liability report.
12. The Ticket/Voucher system shall produce an audit trail message for every user login and logouts.
13. The Ticket/Voucher system shall ensure that no duplicate Ticket/Voucher will be generated by the system.
14. The Ticket/Voucher system shall also comply with any requirements specified by the Casino Operator if it does not contradict the requirements specified in this Standard.

## 4.10 Cashless Systems

### 4.10.1 General

A cashless system may be entirely integrated into a CMS or exist as an entirely separate entity. A gaming machine supporting cashless shall be equipped with a suitable device to read the player identity such as a card reader and a display device for communication to the player at various stages of cashless transactions. The player identification device and the display device will have a communication connection to the cashless system. If the cashless system uses magstripe cards or other approved identification devices for identifying the player, then the same cards or other approved identification devices will be used to support state-wide pre-commitment and must comply with relevant sections of the current *'Victorian Player Account Equipment Technical Requirements Document'*.

### 4.10.2 Player Identification Methods

The cashless system may use different type of methods to identify a cashless player. Some of the possible methods are given below:

1. A magstripe card;
2. A smart card;
3. Identification devices such as 'Dallas Key';
4. The Commission approved digital identification methods; and
5. Biometric identification techniques.

### 4.10.3 Types of Players

Cashless systems generally have the following two types of players – registered players and anonymous or casual players.



#### 4.10.3.1 Registered Players

1. The Casino Operator shall register a player as a registered player only if the Casino Operator is satisfied with the player's identity, place of residence, player's age is at least 18 years and the person is not an excluded person.
2. Unique registered identification methods are only permissible when registering a player.
3. All funds that are considered to be unclaimed as per the relevant legislation shall comply with the '*Unclaimed Money Act 2008*'.
4. The player must set a pin at the time of enabling the player's Cashless account.

#### 4.10.3.2 Anonymous or Casual Player

1. Instead of a registered player, a player may request, and the Casino Operator may issue an anonymous or casual player identification method which is valid for play for a period specified by VCGLR from the date of the last transaction performed using the identification number.
2. Play performed by an anonymous or casual player will not contribute toward any player loyalty/reward scheme offered by the Casino Operator.
3. All funds that are considered to be unclaimed as per the relevant legislation shall comply with the '*Unclaimed Money Act 2008*'.
4. The Casino Operator must set a pin at the time of issuing/re-issuing the cashless access device and the player will have an option to change this pin.

#### 4.10.4 Player Funds

1. Player funds and entitlements, and the player's right to access their funds and entitlements must be preserved and secured against access by persons other than the player unless otherwise authorised by the player in writing.
2. Player funds on the system must be secured against invalid access or update other than by approved methods especially any changes to the player authentication method.
3. The player must not be able to override any set limits or regulatory limits for money transfers.
4. The player must be authenticated every time a deposit or withdrawal to the player account is performed. The authentication methodology and other security arrangements must be demonstrated to be sufficiently robust to prevent unauthorised access to a player's funds and account details.
5. No cash advance or credit play gaming is allowed.
6. Funds from an account associated with a registered or anonymous player may only be used with a gaming provider if that gaming provider had issued the player validation method.
7. The system must be able to display the balance to the player, when requested by the player, for a registered or anonymous/casual account.
8. The system must not accept a request to transfer credits to an EGM that would cause a player's account to become negative.
9. Inactive accounts holding moneys in the system must be protected against forms of illicit access or removal. Balances in both registered and casual player accounts not activated must be handled according to the procedures approved by VCGLR.
10. The cashless system shall have the capability to automatically lock a player account when a specified number of unsuccessful authentication attempts to access the cashless account has been exceeded.
11. The cashless system shall have a capability to flag a player identification method as lost or abandoned. The cashless system must also report when an attempt is made to use a lost or abandoned player identification method.
12. The cashless system shall enforce a maximum balance limit on a player's account (both registered and anonymous/casual players). Any EGM payment that will exceed this maximum balance limit shall be done by other approved methods.
13. The cashless system will not transfer any amount that will exceed the maximum credit balance on the EGM (if applicable).

14. The internal control procedures for issuing of replacement player identification devices and changing of player authentication pins must be secure to prevent any unauthorised access to a player's funds and account details.

#### 4.10.5 Cashless System Requirements

1. The cashless system shall be designed such that the access privileges required to perform different types of user functions shall be associated with different types of user accounts to restrict access to secure and sensitive sections of the cashless system.
2. The cashless system database shall be designed such that all the critical information generated such as player account number, amount etc. shall be stored such that any unauthorised alteration of this information is not possible once it is stored in the database. In the event any financial data is changed, an automated audit log shall be generated to capture the following (at a minimum):
  - a. Identification of the player;
  - b. Data element and value before change;
  - c. Data element and value after change;
  - d. Time and date of change; and
  - e. User (id) that performed the change.
3. The cashless system database shall be designed such that it would limit any potential of system failure and/or loss of information. The cashless system shall be designed to ensure that a power loss or a restart of any node will not result in incorrect account balance.
4. The cashless system shall have the capability to generate daily monitoring logs of user accesses.
5. The cashless system should have the capability to generate a report of all 'funds in' and/or 'funds out' for a given period.
6. The cashless system shall have the capability to generate a report of all cashless transfers in and/or out for a given player and/or with an EGM for a selected period.
7. The cashless system shall have the capability to generate a report of all expired player accounts (if supported). The cashless system shall have the capability to generate a cashless liability report.
8. The cashless system shall produce an audit trail message to a secure log for every user login and logouts.
9. The cashless system shall ensure that no duplicate funds transfer in or out will be generated by the system.
10. The cashless system shall also comply with any requirements specified by the Casino Operator if it does not contradict the requirements specified in this Standard.
11. The cashless system shall have a facility to stop all cashless related activities for a player. Additionally, there shall be procedures to commit or roll back (or adjustments) any transactions in a pending state. The cashless system shall have a capability to produce a report on all commit and/or roll back transactions performed for a given period.
12. As a minimum, the player authentication data (e.g. Pin) must be encrypted in a non-reversible form for storage and use.

#### 4.10.6 Reportable Events

The Casino Operator must keep records of the following events:

1. Player registration, player's account creation and de-activation;
2. Changes to player's registration or account details (e.g. address);
3. Changes made by gaming providers to gaming parameters (e.g. deposit);
4. All transactions made on a player's account;
5. Large transfer of funds as per AUSTRAC requirements;
6. Player exclusion (including exclusion, requests to lift exclusion, and actual lifting of exclusion); when a player attempts to access an account with correct authentication details;
7. When a player's account is locked;

8. When a player's account is locked by the system;
9. When a Casino Operator performs a commit/rollback (or adjustments) transaction including the details of the transaction; and
10. The cashless system shall provide an online search facility that enables comprehensive searching of the event log for all pending and completed cashless transactions for at least the previous thirty (30) days of data. The search facility shall have the ability to perform a search based on at least the following:
  - a) Date and / or Time range;
  - b) Unique gaming machine/kiosk/Cashier's desk identification number; and
  - c) Patron's loyalty membership number.

#### 4.10.7 Display Requirements

As a minimum, the player interface module shall be capable of providing confirmation/denial of every cashless transaction initiated. This confirmation/denial should include:

1. The type of transaction (Credit transfer In and Credit transfer Out);
2. The transaction value;
3. A descriptive message on the success or failure on the transaction initiated; and
4. A message describing the type of error should be displayed to the patron at the player interface module in the event of the following error conditions:
  - a) Invalid PIN (can prompt for re-entry up to maximum allowed);
  - b) If a player initiates a cashless transaction and that transaction would exceed the maximum permissible EGM credit limit; and
  - c) Where a transaction will result in exceeding the maximum permissible credit limit on the player's account.

### 4.11 Cash Redemption Terminals (CRT)

#### 4.11.1 Purpose

This section provides the requirements for the operation of Cash Redemption Terminals (CRT) within the Melbourne Casino.

#### 4.11.2 Introduction

A CRT may be used to support some or all the following capabilities:

1. Redeem Ticket-In for cash;
2. Add cash to card based gaming accounts;
3. Withdraw cash from card-based gaming accounts;
4. Provide short pay receipts/tickets for unpaid amounts;
5. View responsible gaming parameters;
6. Convert player points to credits;
7. Dispense funds for other payments such as jackpot payouts; and
8. Provide note breaking.

#### 4.11.3 Hardware Requirements

1. All CRTs must have a permanently attached identification plate which clearly identifies the manufacturer, model, build date and unique serial number of the machine.
2. The design and construction of the CRT is to be of a sufficient standard to withstand limited abuse, vandalism, or fraudulent activity without compromising the integrity of the equipment.
3. The CRT shall be of a sturdy construction with a locking system which resists any kind of unauthorised entry and protects internal components from any abuse. The CRT banknote storage area must be located and attached in such a manner so that it cannot be easily removed by physical force.

4. Access required for correcting operational lockups such as paper jam, hopper empty etc. will not automatically gain access to the stacker area.
5. All protuberances (e.g. buttons, handles, lights) on a CRT that are accessible to patrons, and attachments to a cabinet (e.g. labels and identification plates) must be sufficiently robust to avoid unauthorised removal.
6. Access to any section of the CRT shall be detected through door sensors. The door sensors shall alert the system when a door has been opened and closed.
7. It shall not be possible to disconnect the communication to the host without accessing a locked area.
8. The CRT shall comply with the Power Supply, Electro Magnetic Interference and Electrostatic Interference specifications given in relevant sections of this document.
9. The coin acceptor, diverter and the bill acceptor used in the CRT shall comply with the specifications given for these components in relevant sections of this document.
10. Touch screens must be accurate, and once calibrated must maintain that accuracy for at least the manufacturer's recommended maintenance period. Touch screens must also be able to be re-calibrated by venue staff.
11. The CRT shall have an on/off switch that controls the mains input to the unit which shall be located in a place easily accessible within the interior of the CRT.
12. The CRT manufacturers are responsible for ensuring that all equipment complies with relevant product and electrical safety statutory requirements under the Victorian State and Commonwealth laws.

#### 4.11.4 Software Requirements

1. CRTs must only perform authorised, correct and legitimate TITO or account-based transactions when dispensing cash for valid tickets or transferring funds to/from player cashless account. All these transactions at the CRT must be authorised by the Monitoring System, and applicable data reported back to the Monitoring System for record keeping.
2. The CRT must support signature checking by the CMS or the TITO/Cashless host. This checking must be performed at least on the following instances:
  - a. when the communication between the CRT and CMS or the TITO host is established (or re-established);
  - b. periodically at least once a day; and
  - c. on demand at any time.
3. All software and firmware related to the critical operation of a CRT must be able to be identified and verified.
4. In instances where a CRT loses connection to the host and is unable to perform Cashless or TITO transactions, it is permissible for CRTs to continue to operate with non-host functions (e.g. note-breaking).
5. CRTs must contain sufficient auditing information to reconcile, at a minimum, all transactions initiated in the previous 24 hours.
6. As a minimum, CRTs must have the capacity to display a complete transaction history for the most recent transaction and the previous 99 transactions prior to the most recent transaction.
7. As a minimum, CRTs must have the capacity to display the last 100 events reported/generated.
8. CRT software must have the facility to detect and log faults or errors with any components integral to the operation of the CRT.
9. Access to internal areas of the CRT should be monitored and logged accordingly.
10. Access to different level of functions shall be protected using different levels of user passwords.
11. In situations where a CRT contains insufficient funds to completely pay out a ticket, the CRT may dispense a Short Pay Receipt/Ticket for redemption at a Cashier only. These receipts/ tickets must not be able to be inserted into TITO systems and used for credits.

12. Short pay receipts/tickets issued by CRTs must clearly display “Short Pay; *Receipt or Ticket*” and “Please see Cashier” and contain the following information: terminal identification, venue name, date and time receipt/ticket was generated, amount paid, amount owing and a reference or authentication code unique to the transaction
13. In situations where a CRT does not dispense coin, the CRT may dispense a ticket for the residual amount that would have otherwise been paid out in coin that can be redeemed and used for credits or redeemed at a cage for coin.
14. The CRT must communicate to the host using a secure method. As a minimum the communication protocol must have capability to detect and act upon communication errors.
15. The CRT must perform a self-check of all executables at least on every power up. It should perform this check periodically (once every day) as well as when communication to the host is lost and restored. The CRT must go into a disable state when any corruption in executables is detected. The CRT must not payout the ticket value unless the ticket is stacked.
16. Each CRT connected to a host system must be uniquely identified by the host.
17. The CRT must be capable of synchronizing its real time clock to the CMS or to the TITO host system.

#### 4.11.5 Artwork Requirements

1. The functions and services provided by the CRT must be clearly communicated to patrons. Written instructions must be grammatically and syntactically correct. The default language presented to patrons must be English.
2. Touch screen button icons must be sufficiently separated to reduce chances of the wrong icon being selected due to mis-calibration or parallax errors.
3. The functions of all physical or touch screen buttons must be clearly indicated, preferably on the button. There must be no hidden or undocumented buttons/touch points anywhere on the screen.
4. Artwork must not give the impression that gambling is a reasonable strategy for financial betterment.
5. CRT display/attract screens are encouraged to have Responsible Gambling messages where possible and must display the current Gambling Helpline contact details.  
(for e.g. “*Gambling too much? For free and confidential advice 24/7 call the Gambling Helpline on 1800 858 858 or visit [gamblinghelponline.org.au](http://gamblinghelponline.org.au)”.)*
6. Artwork must not promote the consumption of alcohol while gambling.

## 5 Jackpots

This section covers the requirements that must be followed for operation of jackpots in the Melbourne Casino.

### 5.1 Jackpot Types

#### 5.1.1 Deterministic Jackpot

A deterministic jackpot is where the probability of winning the jackpot does not remain constant over time when all other variables (e.g. Bet) are held constant. The trigger probability is dependent on previous events in time. The probability that the jackpot will be won usually increases over time. This type of jackpot is often called Mystery jackpot.

An example of a deterministic jackpot is where there is a hidden random target number and a current value that starts typically from zero or from a pre-defined value. For every wager, a fraction of the wager is added to the current value. When the current value reaches the target number, the jackpot is awarded.

#### 5.1.2 Non- Deterministic Jackpot

A non-deterministic jackpot is where the probability of winning the jackpot remains constant for repeated constant bet amounts.

An example of a non-deterministic jackpot is betting on the outcome of game for a jackpot win. This type of jackpots is often called as Progressive jackpot.

#### 5.1.3 Standalone Progressive Jackpot

If a jackpot is only winnable on a single gaming machine, it is considered a Standalone Progressive Jackpot.

#### 5.1.4 Linked Jackpot

If a jackpot can be won on more than one gaming machines attached to the link, it is considered as a Link Jackpot.

#### 5.1.5 Time Based Jackpots

If a jackpot can only be won during a specified period, it is considered to be a time-based jackpot. These are normally mystery jackpots.

#### 5.1.6 Card Based Jackpots

If a jackpot can only be won by players playing with a specific type of card, it is considered to be a card-based jackpot.

#### 5.1.7 Tournament Jackpot

In this type of jackpot, the jackpot prize is awarded based on a specified criteria after all the players have played for a defined period.

#### 5.1.8 Community Jackpot

In this type of jackpot arrangement, more than one EGM enrolled in the jackpot pool can win the jackpot prize based on the jackpot rules.

### 5.1.9 External Jackpot system

In this type of jackpot system, the jackpot control mechanism is external to the EGM software and hardware.

### 5.1.10 Internal Jackpot system

In this type of jackpot system, the jackpot control mechanism is embedded in the EGM software and hardware.

### 5.1.11 Communication Failure

A gaming machine shall disable itself within at least 15 seconds when the communication to the jackpot controller is lost and suspend play if the EGM RTP without the jackpot contribution does not comply with the minimum RTP requirements for EGMs operating in the Victorian Casino.

If the EGM meets the minimum RTP requirements without the jackpot contribution and continues to be in game play, a clear message to notify the player that it is not possible to win a jackpot will be provided.

If the jackpot win determination is by game result, these gaming machines must be de-activated from game play within at least 15 seconds when the communication to the jackpot controller is lost. This is regardless of the EGM's compliance with the minimum RTP requirements for EGMs operating in Victorian Casino.

## 5.2 Mystery Jackpots

### 5.2.1 Jackpot Contributions

1. A gaming machine connected to any jackpot must contribute to the corresponding jackpot pool(s) on every eligible credit wagered that increments the gaming machine turnover (coin in) meter or must contribute to the jackpot pool(s) with a constant probability. The jackpot contribution must be as per defined settings stipulated in the Jackpot game rules displayed to the player and within the approved range of parameters for that jackpot.
2. All contributions to the jackpot must be returned to the players as wins except when the jackpot is decommissioned. If any jackpot is discontinued, the accrual amount of the jackpot including the amount in any other pools (e.g. off-line pool, overflow pool) must be dispersed according to procedure. These transactions must be able to be individually tracked for audit purposes.
3. All contributions received once the jackpot pool has triggered must be applied to the next jackpot pool. No jackpot contributions should be lost.
4. A jackpot prize must not be offered at any time when it cannot be won unless the rules for winning the jackpot prize are clearly displayed to the players.
5. The reset value after a jackpot is won shall not exceed more than 80% of the maximum pool value when added with the other pools such as hidden pool, offline pool, overflow pool etc.

### 5.2.2 Unreasonable Meter Increment

1. Jackpot system must perform unreasonable contribution self-tests on all contributions at every stage of transfer between sub-systems. All unreasonable contributions must not contribute to the jackpot pool and the jackpot system must have the capability to generate an event or log when an unreasonable meter event is detected. This event as a minimum should have the following information:
  - a) Amount of contribution received;
  - b) The identification of the gaming machine that generated the event;
  - c) Jackpot identification (if supported); and
  - d) Date and time in the local format.

2. If there has been an unreasonable jackpot contribution, the jackpot controller shall ignore the invalid data. If there has been an unreasonable jackpot contribution consecutively for more than a predefined value for a given period, the jackpot controller should disable the affected gaming machines. The disabled gaming machines should display an appropriate error message. The “unreasonable contribution” amount shall be set up based on the maximum possible bet for the relevant pool.
3. The Casino Operator shall submit the procedure for enabling EGMs disabled by a jackpot controller due to an unreasonable jackpot contribution to the VCGLR.

### 5.2.3 Jackpot Probability

1. In a linked mystery style jackpot:
  - a. The probability of the player winning the jackpot on any linked EGM must be directly proportional to the size of the bet;
  - b. The proportionality factor must not vary between types of gaming machine and/or games (s) played; and
  - c. There should be an equal chance of winning the jackpot at any time when equal amounts are wagered.
2. The mystery jackpot win event must be based on a random event.
3. The random number generator used to generate the mystery win event shall comply with the requirements stipulated in relevant sections of this document.
4. The jackpot trigger value must be set randomly and must have an equal probability of triggering at any value between the startup amount and the ceiling amount.
5. If the gaming machine RTP without the jackpot contribution complies with the minimum RTP requirements for EGMs for operation in Victorian casinos, the relevant EGM may remain in game play. In this case a clear message must be provided to inform the player that the relevant EGM is not included in the jackpot pool and hence it will not be possible to win a jackpot while playing in this EGM.

### 5.2.4 Mystery Jackpot Win

1. Game play conducted while the gaming machine is offline to the jackpot controller must not lead to a mystery jackpot win in itself when the connection to the jackpot controller is re-established.
2. Mystery jackpot wins must be notified to the winning gaming machine within 3 seconds of the commencement of the game to avoid ‘Player Walk-Away’.

### 5.2.5 Walk - Away

1. ‘Walk-Away’ occurs when a jackpot prize is awarded to an EGM with no player in attendance or if a player mistakenly leaves the EGM not realizing a jackpot is won.
2. The ‘Walk-Away Period’ is defined as the period of time starting the instant a game play is commenced and that results in the player credit meter going to zero, until the time the EGM is awarded and displays to the player any jackpot prize which may occur as a result of the last play contribution.
3. Where Walk-Away is possible, the jackpot system design and performance must:
  - a. Minimize the walk-away period; and
  - b. Not have a walk-away period that exceeds 3 seconds.

### 5.2.6 Internal Linked Mystery Jackpots

For internal linked mystery jackpot systems where the jackpot controller is part of the game software (internal link), all games on the link shall conform to the following criteria:

1. Each game on the link shall be uniquely identified;
2. Only one game at a time on the link shall function as the master progressive controller. This includes links which use Dynamic Master / Slave configurations;



3. If the game configured as the master controller becomes inoperative, all games on the link shall be disabled until another game has been established as Master; and
4. If any game on the link loses communication with the master controller, the game shall be disabled.

### 5.2.7 Parameter Change

1. All modifications to critical jackpot parameters shall be controlled using a secure method.
2. When any critical jackpot parameters of an external jackpot system are modified, the system should have the capability produce a report or through audit logs which shall contain as a minimum the following:
  - a. Date of Parameter Change;
  - b. Person making the change;
  - c. Parameter values before the modification; and
  - d. Parameter values after the modification.

## 5.3 Progressive Jackpots

### 5.3.1 Jackpot Contributions

1. A gaming machine connected to any jackpot must contribute to the corresponding jackpot pool(s) on every eligible credit wagered that increments the gaming machine turnover (coin in) meter or must contribute to the jackpot pool(s) with a constant probability. The jackpot contribution must be as per defined settings stipulated in jackpot game rules displayed to the player. Prior approval from VCGLR shall be obtained for any jackpot implementations that do not comply with this requirement (VCGLR will require details of the proposed methods for jackpot reconciliation in such arrangements).
2. All contributions to the jackpot must be returned to the players as wins except when the jackpot is decommissioned. If any jackpot is discontinued, the accrual amount of the jackpot including the amount in any other pools (e.g. offline pool, overflow pool) must be dispersed according to a procedure.
3. All contributions received once the jackpot pool has triggered must be applied to the next jackpot pool. No jackpot contributions should be lost.
4. If a ceiling value is established on a jackpot, all additional contributions once that cap is reached are to be credited to an overflow pool.
5. A jackpot prize must not be offered at any time when it cannot be won unless the rules for winning the jackpot prize are clearly displayed to the players.
6. Each gaming machine on the link shall have the same probability of winning the jackpot up to 14 decimal points, for the same denomination played.

### 5.3.2 Unreasonable Meter Increment

1. Jackpot system must perform unreasonable contribution self-tests on all contributions at every stage of transfer between sub-systems. All unreasonable contributions must not contribute to the jackpot pool and the jackpot system must generate an event when an unreasonable meter event is detected if supported. This event as a minimum should have the following information:
  - a) Amount of contribution received;
  - b) The identification of gaming machine that generated the event;
  - c) Jackpot identification (if supported); and
  - d) Date and time in the local format.
2. If there has been an unreasonable jackpot contribution, the jackpot controller shall ignore the invalid data. If there has been an unreasonable jackpot contribution consecutively more than a predefined value for a given period, the jackpot controller should disable the affected gaming machines. The disabled gaming machines in the group should display

an appropriate error message. As a minimum the unreasonable amount of credits bet value shall be set up based on the number of bets and number of machines.

3. The Casino Operator is required to have a procedure for enabling the EGMs after it has been disabled by a jackpot controller due to an unreasonable jackpot contribution.

### 5.3.3 Simultaneous Wins

1. In a progressive jackpot system, it is possible to have simultaneous wins where two or more players have won the same jackpot pool on different gaming machines. Under this condition, either of the following two options shall be supported:
  - a. The first gaming machine that reported the jackpot win to the jackpot system is paid the current jackpot pool value and the second gaming machine that reported the jackpot win is paid with the jackpot reset amount including any contributions from the overflow pool, diversion pool, hidden pool etc.
  - b. All the eligible winners are paid the jackpot pool value in full.
2. To minimize the probability of simultaneous jackpot wins, the progressive controller must give the highest priority to resetting the jackpot pool after a jackpot hit.
3. The Casino Operator is required to have a procedure for handling simultaneous wins. The procedure is for dealing with the possibility of a jackpot being won (or appearing to be won) by one or more players at approximately the same time.

### 5.3.4 Jackpot Wins When Communications Go Down

In a progressive jackpot system, it is possible to have a jackpot win on a gaming machine when the communication between the gaming machine and the jackpot controller is lost. The Casino Operator is required to have a procedure for handling jackpot wins when communication to the jackpot controller is lost.

### 5.3.5 Internal Link Progressives

For internal link progressives where the progressive controller is part of the game software (internal link), all games on the link shall conform to the following criteria:

1. Each game on the link shall be uniquely identified;
2. Only one game at a time on the link shall function as the master progressive controller. This includes links which use dynamic Master / Slave configurations;
3. If the game configured as the master controller becomes inoperative, all games on the link shall be disabled until another game has been established as Master; and
4. If any game on the link loses communication with the master controller, that game shall be disabled.

### 5.3.6 Parameter Change

1. All modifications to jackpot parameters shall be controlled using a secure method.
2. When any critical jackpot parameters of an external jackpot system are modified, the system should have the capability to produce a report or through audit logs which shall contain as a minimum the following:
  - a) Date of parameter change;
  - b) Person making the change;
  - c) Parameter values before the modification; and
  - d) Parameter values after the modification.

## 5.4 Jackpot controller requirements

The requirements specified in this section are applicable to both mystery and progressive linked jackpot systems.

### 5.4.1 General

Jackpot controller means hardware and software that controls communications among the various devices connected to the jackpot system, calculates the values of the jackpots pools and displays all the relevant information within a gaming device linked to the jackpot and/or on the associated jackpot display.

### 5.4.2 Physical

If the jackpot controller is not located within the secure computer room, the jackpot controller shall comply with the following requirements:

1. The jackpot controller shall be housed in a secure environment allowing only authorised accessibility.
2. The jackpot controller shall comply with the applicable requirements specified in the relevant sections of this document.

### 5.4.3 Critical Memory

1. Jackpot controller critical memory shall be implemented as specified in relevant sections of this document if a Jackpot controller uses critical memory as per the manufacturers design.
2. All jackpot controller parameters and meters shall be stored in the critical memory if a Jackpot controller uses critical memory as per the manufacturers design.

### 5.4.4 Monitoring of Credits Bet

The jackpot controller shall continuously monitor each gaming machine in the group for credits bet and update all meters timely and accurately.

### 5.4.5 Jackpot Configuration

1. The method by which system jackpot parameter values are entered or modified is to be secure.
2. All jackpot controllers shall display, upon request, the following information for each jackpot prize offered (if applicable):
  - a. Jackpot Type: Type of jackpot prize paid such as Current Pool value, Fixed amount, non-cash prize etc.;
  - b. Start Up: Starting value of the jackpot pool;
  - c. Ceiling Value: Jackpot limit value (The contributions received from the connected gaming machines when the jackpot has reached this limit will be added to the overflow pool);
  - d. Reset Value: The amount the jackpot resets to after the jackpot is won;
  - e. Increment Percentage: Percentage increment rate for the pool;
  - f. Hidden or Reserve Increment: Percentage increment rate for hidden or the reserve pool;
  - g. Current Pool value: Current prize amount;
  - h. Overflow Pool value: Amount contributed after the jackpot has reached the limit;
  - i. Hidden or Reserve Pool Value: Amount contributed to the hidden or reserve pool;
  - j. Win History: History of a minimum of the last 25 jackpot hits;
  - k. Total Wins: Value of total jackpot wins paid for this jackpot pool within the stored memory of the Jackpot controller as per the manufacturers design;
  - l. Total Contribution: Value of total credits bet received for this jackpot pool; and
  - m. Contributing EGMs: Details of the participating gaming machines;
3. If the jackpot controller is capable of configuring additional pools and/or increments, all parameters pertaining to these shall similarly be displayed upon request.
4. While a jackpot group is in operation, no parameter changes may take place, unless for situations listed in the Internal Control Procedures of the casino.
5. All amounts in the hidden pools shall be returned to player.

#### 5.4.6 Error Conditions

1. When a jackpot controller error occurs, an appropriate error message shall be made visible to all the players affected by the error, and the Casino Operator shall be alerted of the error condition.
2. The jackpot controller shall convey the appropriate signal to disable all the gaming machines in the appropriate jackpot group and an error shall be displayed on the jackpot display and all the gaming machines in the group when an error occurs.
3. If the error and events are not reported online to the CMS, the jackpot controller shall retain at least the last 100 events and errors.

#### 5.4.7 Meter Rollover

1. The jackpot controller shall handle EGM credits bet meter rollover without corrupting any jackpot pool value and the jackpot must remain auditable.
2. If it is possible for any meters in the jackpot controller to rollover during the life of the jackpot, then this must be handled transparently. The current jackpot amount must never be corrupted, and the jackpot must remain auditable.

#### 5.4.8 Program Interruption and Resumption

1. After a program interruption (e.g., power down), the software shall be able to recover to the state it was in immediately prior to the interruption occurring.
2. On program resumption, the following procedures shall be performed at the minimum:
  - a. Any communications to an external device shall not begin until the program resumption routine, including self-tests, is completed successfully;
  - b. The integrity of all critical memory shall be checked if a Jackpot controller uses critical memory as per the manufacturers design.

#### 5.4.9 Independent Software Verification

The jackpot controller software used within a linked jackpot group shall allow for an independent integrity check of the control program from an outside source.

#### 5.4.10 Interface to CMS

The jackpot controller shall support a capability to enable CMS to get all relevant jackpot parameter values as specified in the section 'Jackpot Configuration'.

#### 5.4.11 Signature Verification

The jackpot controller shall support a capability for the signature checking of its software by the CMS or another trusted device. All signature verification methods used shall meet the requirements stipulated in relevant sections of this document or better.

#### 5.4.12 Jackpot Display

1. Jackpot displays must have the capability to display the current amount of the jackpot(s), which must be updated accurately and as often as possible so as to reasonably reflect the current size of the prize pool. When a jackpot prize is won then the display must "catch up" to the precise value of the jackpot won.
2. If more than one win occurs for a jackpot at approximately the same time, all such jackpots wins must be shown on the jackpot display. It is not acceptable to overwrite the first win with the second without a minimum reasonable display period of 30 seconds. A jackpot display rotating through showing all the current jackpot wins is acceptable.

3. If no jackpot display capability is operating for a jackpot (i.e. all methods of displaying the current jackpot amount to participants of the jackpot have stopped operating) the jackpot must be shutdown either manually or automatically in a reasonable amount of time.
4. If the power of jackpot controller is down, the jackpot display shall show a message similar to "Link Down" to all players.
5. On power up, a jackpot display system should not display current amounts until the current amounts have been updated by the jackpot controller/progressive system. This is to avoid displaying out of date values for the current amounts.

### **5.4.13 Jackpot Win**

#### **5.4.13.1 Jackpot Win Notification**

1. The following indications for the winning of a jackpot prize are required:
  - a. Audible on selected jackpots;
  - b. Visual indication of such an event on the winning gaming machine; and
  - c. Visual indication of the win on the main jackpot display, unless all the information on the display is available on all the participating gaming machines.
2. The jackpot controller shall be able to send the winning gaming machine the amount that was won.
3. The notification of the winning of any jackpot must be passed by electronic means to the winning gaming machine.
4. When a jackpot win is recorded on a gaming machine, which is attached to the jackpot controller, the controller shall allow for the following to occur on the jackpot display:
  - a. Display of the winning amount and a visible notification to inform the player(s) who won the jackpot; and
  - b. Display of the new jackpot values of each level that are current on the link after a reset of the current jackpot amount.
5. When a jackpot win is paid, the jackpot controller shall record an event with the following details:
  - a. Jackpot amount or prize paid;
  - b. Details of the EGM for which the jackpot was paid;
  - c. Date & time; and
  - d. Method of payment (Paid to the credit meter or hand pay voucher).
6. If the jackpot controller is communicating online to the CMS, all the above information shall be transmitted to the CMS.
7. Jackpot controllers may be connected to a database server that enables accounting data to be extracted as reports.
8. The jackpot controller shall have the capability to be configured with a limit on each jackpot prize offered.
9. If the jackpot has to be reset manually, the method of "Resetting" the jackpot display so as to no longer show the last win details must be secure.

#### **5.4.13.2 Winning Gaming Machine**

When a jackpot prize has been awarded, the winning gaming machine shall perform the following:

1. Display the winning prize;
2. Unless the jackpot award is transferred to player's credit meter, the game software and the machine shall lock-up entirely and require intervention by an attendant; and
3. All jackpot related meters shall be updated to reflect the winning jackpot amount.

#### **5.4.13.3 Reset of Jackpot Amount**

1. The jackpot controller shall have the ability to reset the current jackpot amount to the startup value with the addition of any applicable amount from hidden pool(s) (if applicable) after a jackpot prize has been awarded.

2. If the reset of the jackpot amount is manual, then the method of reset shall conform to the Casino Operator's internal controls procedures.
3. If the reset of the jackpot amount is automatic, then all the gaming machines on the link shall continue normal play after the reset.

#### **5.4.14 Jackpot Shutdown**

There are instances where a jackpot group may be temporarily shut down. Such a jackpot shutdown requires the following actions:

1. Clear indication shall be given to the players that the relevant jackpot group is currently not operating;
  - a. It shall not be possible for the jackpot to be won while in the shutdown state; and
  - b. Activation of the jackpot group from the shutdown state shall return the group with the identical parameters as before the shutdown.
2. If the jackpot win determination is by a game result, these gaming machines must be de-activated from game play until the jackpot is re-activated.

#### **5.4.15 Reporting Requirements**

The jackpot controller shall be capable of generating reports. In instances where the central jackpot server is in constant communication to another system such as a CMS, these jackpots related reports may be generated from the CMS.

#### **5.4.16 Time Synchronization**

1. The jackpot controller shall maintain an internal clock that accurately reflects the current time (in hours, minutes and seconds) and date that shall be used to provide for the following:
  - a) Time stamping of significant events;
  - b) Reference clock for reporting; and
  - c) Time stamping of configuration changes.
2. The jackpot controller shall support capability to synchronizing time with an external reference clock.

### **5.5 Tournament Jackpots**

#### **5.5.1 Activation of Tournament Mode**

1. The switching between tournament mode and live gaming mode shall be tracked. At the minimum, the following events shall be logged:
  - a. Time of the switch from live gaming mode to tournament mode;
  - b. Start time of the tournament;
  - c. End time of the tournament and end time of each session during the tournament mode;
  - d. Number of tournament sessions played during tournament mode;
  - e. Game title played for each session;
  - f. Mode of each session (time only, credit only or both) and
  - g. Time of the switch from tournament mode back to live gaming mode.
2. The gaming machine shall complete any game, credit transfer or other transactions (e.g. bill, coin, cashless, ticketing etc.) prior to entering the tournament mode.
3. The gaming machine shall not enter tournament mode while credits exist on the gaming machine.

### 5.5.2 During Tournament Mode

1. All coin and banknote acceptor devices or equivalent shall be disabled when the gaming machine is placed in tournament mode. Cards (or other devices) used for cashless gaming shall not be able to be used to facilitate the transfer of credits to or from a gaming machine in tournament mode.
2. The cash out button or equivalent shall be disabled while the gaming machine is in tournament mode.
3. Tournament credits shall have no cash value and shall be used solely to establish player rankings at the end of a tournament session.
4. All accounting meters and history data, except those intended solely for tournament mode tracking, shall be preserved upon entering the tournament mode and must be restored upon exiting the tournament mode.
5. The gaming machine shall not communicate any non-tournament mode accounting information to the CMS during tournament mode.
6. A message indicating that the machine is in tournament mode must be clearly displayed on the machine.
7. Linked progressives, linked mystery and standalone progressives shall not form any part of tournament play.
8. All gaming machines designed for the same tournament game play shall be able to run identical software on the same hardware electronics and be configured with the same machine settings including reel speed settings, hit rates, max bet limits and bonus games.

### 5.5.3 Submission Requirements

1. The procedures for the conduct and playing of tournament games are to be included in the internal controls and procedures manual which shall require the approval of VCGLR.
2. As a minimum, a submission to VCGLR shall include details for the following:
  - a. Conditions of entry and fees;
  - b. Prize pool and distribution;
  - c. Conditions of play; and
  - d. The requirements for "Tournament Mode" operation of gaming devices.

### 5.6 Community Style Jackpots

In a 'community style' jackpot, a number of EGMs participate in a jackpot feature and the jackpot prize is awarded to some or all of the EGMs based on the jackpot payment rule. The following provides specifications for implementing such jackpot types:

1. The jackpot prize can only be awarded to the contributing EGMs that are part of the community style linked jackpot arrangement;
2. The jackpot prize must be distributed according to the jackpot payment rule;
3. The effective increment rate of a jackpot prize pool shall be submitted to VCGLR for approval;
4. An EGM eligible for a jackpot award must have contributed to the jackpot pool in accordance with the configured amount of time on the system from the end of a game that contributed to the jackpot pool;
5. The parameter sets submitted to VCGLR for approval of a community style jackpot shall contain the number of jackpots that can be won concurrently including the start-up and maximum preset values (if applicable);
6. The community style jackpot systems shall provide as a minimum the following advice to the players:
  - a. A statement that an EGM not played up to the configured period prior to a jackpot being triggered shall not be awarded a jackpot.
7. Jackpot audit and event data must include the history of each individual jackpot prize won; and

8. The jackpot system shall have capability for jackpot accounting reconciliation.

## **5.7 Communications**

The requirements specified in this section are applicable to both mystery and progressive linked jackpot systems.

### **5.7.1 Between Jackpot Controller and Electronic Gaming Machines**

1. There shall be a secure, two-way communication protocol between the main game processor board on the gaming machines and the jackpot controller.
2. The jackpot controller shall send to the electronic gaming machine the amount that was won for metering and/or display purposes.
3. For a game determined jackpot, the winning electronic gaming machine shall inform the controller that a win is triggered.
4. The jackpot controller shall continuously update all electronic gaming machines in the group with the current jackpot prize pool.

### **5.7.2 Between Jackpot Controller and Jackpot Display**

1. There must be a reliable communication protocol between jackpot display and jackpot controller.
2. The jackpot controller shall continuously update the jackpot display as play on the link is continued. This communication protocol shall be secure.
3. The jackpot display must not indicate incorrect jackpot pool value when the communication between jackpot display and jackpot controller is lost and must indicate clearly that the jackpot is not functional under this condition.



## 6 Table game requirements

### 6.1 Electronic Table Game requirements

Electronic Table Games (ETG) games can be classified into the following two types:

1. A Semi-Automated Table Games (SATG) Means a Table Game which comprises multi-terminal stations that access and have connectivity with a base unit, but which still deliver the game using any mechanical or manual device (including all such semi-automated versions of games identified in clause 27.1 of the Casino Agreement).
2. A Fully Automated Electronic Table Games (FATG) Means a Table Game which comprises multi-terminal stations that access and have connectivity with a base unit that is delivered via the use of a fully automated, animated or electronic system with no part of any mechanical or manual device remaining (including all such fully automated, animated or electronic versions of games identified in clause 27.1 of the Casino Agreement).

#### 6.1.1 Common Requirements

SATGs and FATGs shall comply with the requirements specified in this section.

##### 6.1.1.1 Applicability of the Technical Standards

SATGs and FATGs shall comply with the requirements stipulated in this document wherever applicable.

If the integrity of the game in play is not compromised, it is permissible to disable just the terminals affected by any errors and allow gaming to continue on unaffected terminals.

##### 6.1.1.2 Game Rule

1. All game rules and payout must not deviate from the corresponding official game rules approved by VCGLR;
2. The terminals must provide a means of displaying the rules of the game, game outline and collection schedule, and the prize that will be paid to the player when the player obtains a specific win;
3. The video display shall clearly indicate whether awards are designated in denominational units, currency, or some other unit as provided for in the Rules of the game or approval granted by the Commission;
4. All pay table information must have an option to be presented to the player, prior to them committing to a bet;
5. The game being played must at all times be clearly visible to the player; and
6. Each individual bet to be played shall be clearly indicated on the player interface so that the player is in no doubt as to which wagers have been made.

##### 6.1.1.3 Mandatory Credit Return (Forced Bet)

The terminal should reject and return the credits wagered by the player if the credits bet is less than the minimum bet value for the selected bet option (e.g. a roulette game that has different minimum bet values for different types of bet types).

##### 6.1.1.4 System Clock

The SATGs and FATGs shall maintain an internal clock that accurately reflects the current local time and date that shall be used to provide for the following:

1. Time stamping of significant events;
2. Reference clock for reporting; and
3. Time stamping of configuration changes.

If multiple clocks are supported, the SATGs and FATGs shall be capable of maintaining and synchronizing the time for all clocks in each system component so as to ensure that time stamping of all events and data is correct.

The SATGs and FATGs shall have a capability for synchronizing time with an external reference clock.

#### 6.1.1.5 Player Interface Terminal Requirements

The player interface terminal(s) must comply with all the relevant hardware and software requirements specified in relevant sections of this document.

#### 6.1.1.6 Player Interface Error Circumstances

The Player Interface terminal shall be capable of complying with all the relevant faults and errors requirements specified in relevant sections of this document including reporting and displaying of the error together with the remedial action to be taken to clear the event.

#### 6.1.1.7 Game Recall

##### 6.1.1.7.1 Game Recall (Terminals)

1. For the Game Recall information held by each terminal in a multiple terminal environment, it must be possible to show to the player the results of the play(s) as the player originally saw it. The manner in which the information is provided must enable observers to clearly identify the game sequences and result(s) that occurred.
2. Information on at least the last ten (10) games played on the terminal is to be always retrievable through the operation of a suitable key-switch, or another secure method that is not available to the player.

##### 6.1.1.7.2 Game Recall Information Required

The game recall screen shall, as a minimum, be capable of showing the following information:

1. Card values, balls drawn or other form of game result;
2. Total number of credits at the start of play (less credits bet);
3. Total number of credits at the end of play;
4. The total number of credits bet including details of the bet made by the player;
5. The total number of credits won associated with the prize resulting from the last play and the value in dollars & cents for progressive prizes, if applicable;
6. The total number of credits added (separated into coins, bills and cashless) since the end of the previous play and through to the end of the last play;
7. The total number of credits collected (separated into coins, vouchers and cashless) since the end of the previous play and through to the end of the last play;
8. The total value of cancelled credits (in dollars & cents) since the end of the previous play and through to the end of the last play (credits added or collected after the last play will be recorded on the completion of the next play);
9. Any player choices involved in play outcome including cards held, balls selected, etc.; and
10. The value of all Standard Meters (as defined in Section '*Master Meters*' in this document) as at the end of the last play. Specific meters that are not applicable, may be omitted.

Note: The above requirements are the default for Last Play Information in that events after the completion of the last play (such as inserting money to add credits or collecting credits) do not form a part of the last play requirements. However, it is permissible for manufacturers to display this information provided it is clear what happened after the completion of the last play.

#### 6.1.1.8 Game Play Information

A terminal in a multiple terminal setup must display the following information to the player at all times when the machine is available for player input:

1. The current credit balance;
2. The current bet amount;
3. The amount won for the last completed game (until the next game starts or the betting options are changed);
4. The results for the last completed game shall be clearly indicated to the player (until the next game starts);
5. The current time of the day; and
6. The denomination of the game being played.

#### 6.1.1.9 Artwork

1. There must be sufficient information to allow a player to determine the correctness of prizes awarded.
2. The payable applicable to the device must be clearly visible, or the means of displaying such information must be readily available to the player prior to committing to a bet.
3. All statements on the artwork must be true.
4. Written messages displayed shall be both grammatically and syntactically sound in the language. If a language other than English is available, the player must be able to toggle between the other language and English. The default language used to display the messages shall be English.
5. The display of the result of a game outcome must not be misleading or deceptive to the player
6. The message "Malfunction Voids All Pays and Play" or its equivalent must be displayed on each terminal in a multiple terminal setup.
7. The game instructions must be clearly visible, or the means of displaying such instructions must be readily available to the player prior to committing to a bet and when the terminal is waiting for player input.
8. All game instructions on the artwork must be easily interpreted, not ambiguous, and sufficient to explain all game rules.

#### 6.1.1.10 Significant Logs and Events

All relevant significant events as specified in this document produced by the terminal shall be sent directly to the CMS utilizing a Communication Protocol supported by the CMS.

The Casino Operator shall have the capability to record, store and monitor all relevant significant events that occur at each terminal and server if supported by the CMS. Access to change any event or log history must be controlled with the appropriate System Administrator access privileges in accordance with supervised access controls.

The Event History may be divided into sections; these events will be logged by date, time and event. Each event must be stored in a database(s) which contains the following:

1. Date and time which the event occurred;
2. Identity of the system element that generated the event;
3. A unique number/code that identifies the event; or
4. A brief description that explains the event.

#### 6.1.1.11 Accounting Information

The terminals must transmit all the relevant meters required to the CMS for appropriate revenue reporting and auditing.

### 6.1.1.12 Report

Terminals shall transmit all financial information and relevant significant events information in real time to the CMS so that the CMS can retain all this information and can produce the desired reports on demand.

## 6.1.2 System Requirements

### 6.1.2.1 System Redundancy

The server should have sufficient redundancy and modularity so that if any single component or part of a component fails, no gaming data is lost. There shall be redundant copies of each log file or system database or both on the system with support for backups and restoration.

### 6.1.2.2 Backup & Recovery

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

1. Information on system configuration;
2. Significant Events;
3. Account information including winnings, bets, cash deposits and cash withdrawal;
4. Audit information;
5. Specific site information such as Device file, employee file, game profiles, etc.;
6. Game Play statistics; and
7. Current system encryption keys.

## 6.1.3 System Security

### 6.1.3.1 Physical Access

The server or system element(s) must be located in a secure locked area where access is limited to authorised personnel. If supported, logical access to the server must be logged on the system or on a computer or other logging device that resides outside the secure area. The logged data should include the date, time and the identity of the individual accessing the secure area. The resulting logs should be kept for a minimum of 100 days.

### 6.1.3.2 Data Amendment

The system shall not allow the amendment of any accounting or significant event log information without supervised access controls. In the event financial data is amended, the audit log must record:

1. Date and Time of amendment;
2. Data element value prior to amendment;
3. Data element value after amendment;
4. Data element amended; and
5. Personnel that performed amendment (by username/ID).

### 6.1.3.3 Access Control

1. Role Based Access Control whereby users are only allowed access to programs and menu items related to their job functions shall be supported.
2. A record of all privileges allocated to user accounts shall be maintained.
3. All passwords, PINs, biometrics or other electronic forms of identity information, if used as part of the authentication method, shall be encrypted in storage.
4. There shall be a non-alterable audit trail of all user logon activities.

5. There should be a provision for system administrator notification, user lockout and audit trail entry after a set number of unsuccessful login attempts.
6. The system shall record date and time of the login attempt, username supplied and a status to indicate if the attempt was successful.
7. The use of generic user accounts on servers is not permitted.

#### 6.1.4 Multi-Games

In multi-game, players have a choice to select a game to play from a given number of games. The following requirements apply to these types of games:

1. There shall be a clear indication to the player about the game options available for play;
2. The player shall be able to review the information on all the games available for play without the need to place a wager;
3. The terminal shall unambiguously indicate the game being selected for play once the player makes a selection;
4. The selection of games shall be available only when the current game being played is completed; and
5. The terminal shall display any residual credit left when a player has an uneven credit left on the terminal.

#### 6.1.5 Communication Protocol

1. All protocols must use communication techniques that have proper error detection and/or recovery mechanisms which are designed to prevent unauthorised access or tampering by employing suitable encryption algorithms.
2. The terminal must support the protocol specified by the CMS to transmit all the financial and significant information to the CMS.

#### 6.1.6 FATG Requirements

The following requirements are applicable only to FATGs:

1. The Random Number Generator (RNG) used to determine the game results shall comply with all the requirements specified for RNG in relevant sections of this document.
2. Any table game which employs multiple decks of cards should alert the player to the number of card decks in play.
3. All FATG terminals shall have the capability to display Electronic Information for players (Player Information Display (PID)) as specified in relevant sections of this document.
4. Players of FATGs must have access to player activity statements showing their play history and the capacity for players to set time and loss limits.

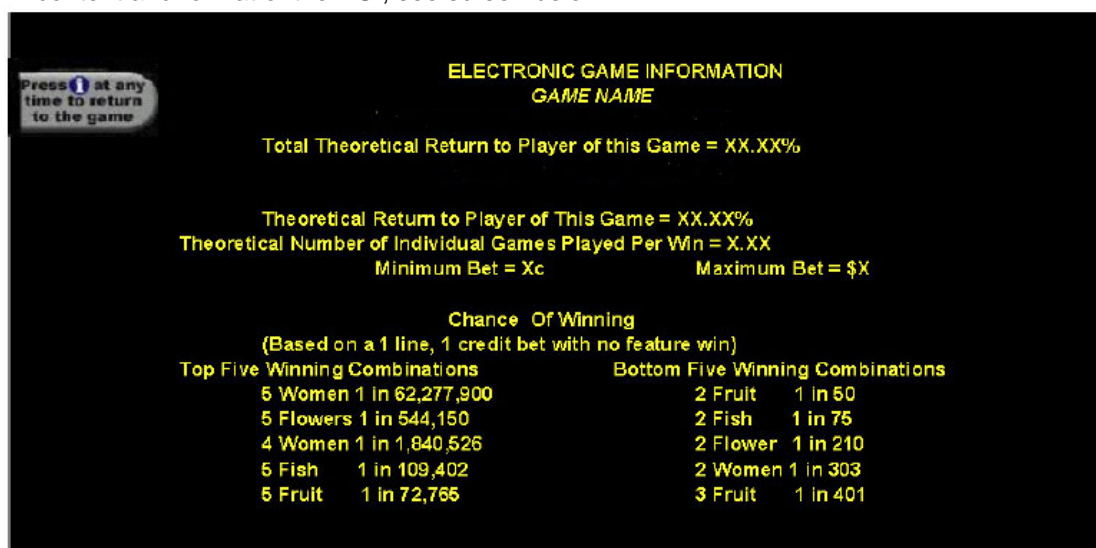
##### 6.1.6.1 Electronic Information for Players for FATG

The requirements for the electronic display of information are laid down in the prevailing Regulations. This includes the display of electronic game information, electronic player information and the time of day. At the time of issue of this version of the TRD, the requirements for electronic game information as stated in the Regulations are:

- A. *What is electronic game information?*  
*Electronic game information* means the following information in relation to a game that may be played on a FATG -
  - a) the return to players of that game;
  - b) the average number of individual games played for each win, based on one line being played per game, which may be described as "theoretical number of individual games played per win";
  - c) the odds of achieving the 5 most valuable individual winning combinations;
  - d) the odds of achieving the 5 least valuable individual winning combinations;
  - e) the maximum and minimum bet options available;

The following interpretations are to be used in conjunction with the requirements for electronic game information:

- if a game operates with more than one Return to Player or with a range of RTP, the range of RTPs' must be displayed.
- where the average number of individual games played per any win, based on one line being played per game, is not possible, the average number of individual games played per any win, can be based on the minimum bet per game play.
- In relation to the chances or odds of achieving the top 5 and bottom 5 winning combinations, where more than one symbol pays the same amount, either the order by chance, hierarchy or alphabetical value can be used for display. For example, if five "Tens" and five "Queens" pay the same amount the "Queens" combination may be displayed first. Similarly, if five "Apples" and five "Oranges" pay the same amount the "Apples" may be displayed first.
- If an automatic timeout period is implemented for displaying the electronic game information, the timeout period must not be less than 30 seconds. For example, the content and format of the EGI, see screen below.



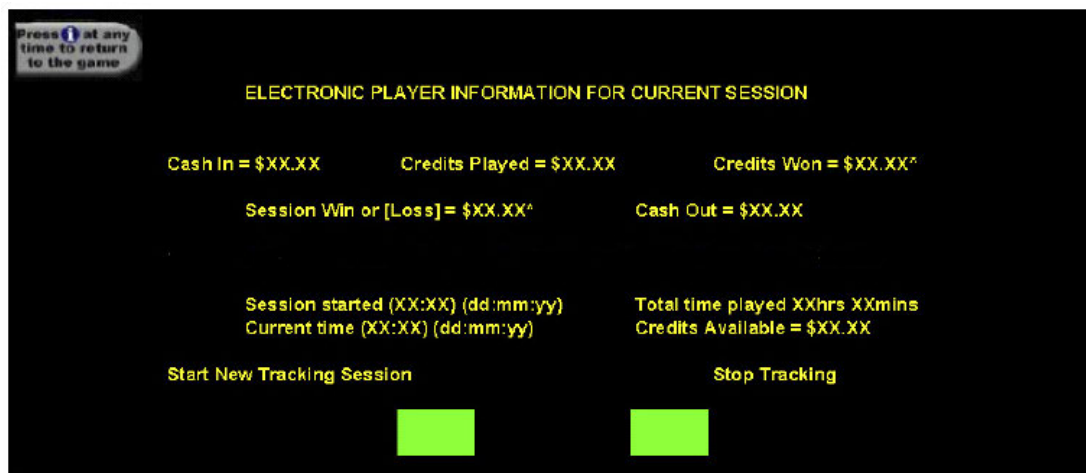
**B. What is electronic player information?**

Electronic player information means the following information in relation to a continuous period of gaming on a FATG by an individual player –

- the amount of money the player has put into the FATG during the period, which may be described as "cash in";
- the amount of money wagered by the player on the FATG during the period, which may be described as "credits played";
- the amount of money won by the player on the FATG during the period, which may be described as "credits won";
- the difference between the credits won and the credits played during the period, which may be described as "session win or loss";
- the amount of money paid out by the FATG during the period which may be described as "cash out";
- the amount of money that is currently available for the player to wager on the FATG, which may be described as "credits available";
- the time at which the period started;
- the current time of day;
- the length of the period;

The following interpretations are to be used in conjunction with electronic player information requirements:

- if an automatic timeout period is implemented for displaying the electronic player information, the timeout period must not be less than 60 seconds.
- See below for an example of acceptable content and format for the electronic player information screen.



### 6.1.7 SATG Requirements

The following requirements are applicable only to SATGs:

- In the event of a discrepancy between the terminal outcome on the video display and the table outcome, the table outcome will be the official result.

## 6.2 Non – Electronic Table Game requirements

The following section describes the requirements of the electronic components utilised in the conduct of gaming and monitoring of table games at the Casino.

### 6.2.1 System Requirements

Software or hardware components utilised in relation to the conduct or monitoring of gaming on table games at the Casino, shall comply with relevant sections of this document.

At a minimum, key requirements/functions of the software or hardware components should include the:

- Following electronic transactions –
  - Opening and closing of tables
  - Chip fills
  - Chip credits
  - Patron chip transfers; and
  - Issuing and acknowledging chip purchase vouchers.
- Primary source of storing data in relation to the gaming activities, and
- Structured reporting only from the primary data source utilised in relation to the ongoing monitoring of gaming activities.

### 6.2.2 Table Interface Devices Requirements

On-table gaming management devices and connected peripherals shall comply with relevant sections of this document.

### 6.2.3 Jackpot Systems

Jackpot systems utilised on table games shall comply with relevant sections of this document.

#### **6.2.4 Display Units**

The display units utilised in the conduct of table games that provide real time data shall comply with relevant sections of this document.

#### **6.2.5 Communication Protocol**

All protocols must use communication techniques that have error detection and/or recovery mechanisms, which are designed to prevent unauthorised access or tampering by employing suitable encryption algorithms.



## 7 Player Promotion / Bonusing System

### 7.1 Overview

The following requirements shall only apply to Player Promotional/ Bonusing systems that can affect the financial settlement such as e.g. redemption of player loyalty points as credits to the player account (which can be used as machine credits) or bonus awards which are paid directly to the EGM credit meter.

All promotional/bonusing credits given to the player have no impact on the calculation of theoretical payback percentage for a gaming machine. Provisions must be made to ensure that these awards are metered uniquely by the electronic gaming machine, so that they can be reported correctly to the CMS for calculation of revenue and promotional/bonus awards reconciliation purposes.

### 7.2 Player Promotion Systems

A Promotional System is typically comprised of gaming devices that are configured to participate in electronically communicated promotional award payments from a host system. The host system controls the promotional award issuance parameters as well as the awarding of promotional credits. Promotional awards are additional elements that entitle players to special promotional awards based on the patrons play activity. Promotional awards are based on predefined patron play activity associated with a specific patron/account.

Static promotional awards are based on predefined criteria that do not require patron gaming machine activity prior to redemption and are generally for single instance use.

The Player Promotion may include for example:

- a) A player may be awarded 100 points for every \$100 played on the gaming machine. These points may then be converted to machine credits at the gaming machine with a point to credits conversion ratio set in the player promotion host;
- b) A player who has established a qualification for gaming machine play activity will be awarded a certain number of machine credits upon returning the next day (or any defined period); or
- c) A player will be given a predefined credit when they first sign up for participating in the player promotion.

The promotional awards/credit in this context are referred to as “free play / match play credits” (i.e. player must contribute money first via gaming machine play to redeem the promotional awards).

### 7.3 Bonusing Systems

Bonusing Systems are typically comprised of gaming devices that are configured to participate in electronically communicated bonus award payments from a host system. The host system controls the bonus award issuance parameters as well as awarding of the bonus payments. The bonus host system provides designated gaming devices with additional elements that entitle players to special Bonus Awards based on events triggered by the gaming device. Bonus awards are those based on a gaming machine event or some external trigger which do not include triggers based upon specific patron account activity.

The Player Bonusing may include for example:

- a) Multiply wins with a specified value for a specified period on participating gaming machines; or
- b) A small bonus prize given to all players playing on gaming machines when a large jackpot is won.

## 7.4 Player Promotion System Requirements

### 7.4.1 Player Information Privacy

1. Use of player information must not breach any relevant state and federal privacy legislation.
2. Any information obtained in respect of player account establishment must be kept confidential, except where the release of that information is required by law or approved by the registered player.
3. Any information about the current state of player account(s) or player activity must be kept confidential except where the release of that information is required by law or approved by the registered player.
4. 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.
5. Data management must be in accordance with the Privacy and Data Protection Act 2014 (Victoria) and the Privacy Act 1988 (Commonwealth).
6. 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.

### 7.4.2 Player accounts maintenance

1. Storage of account data must be secured against invalid access or update
2. All adjustment transactions are to be maintained in a system audit log.  
[www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf](http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf).
3. All transactions involving a player's account data are to be treated as vital information to be recovered in the event of a failure.
4. Personal information of the registered player should 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'.

### 7.4.3 Database Security

Player information, player entitlement and transactions must be secure at all times (e.g. prevention of unauthorised access).

### 7.4.4 Display Notification

Player shall be suitably notified, as a minimum, of the following events on the gaming device and/or interface display element:

- (a) Entry and exit from player loyalty mode (i.e. Indication of promotion participation - availability or unavailability, expiry, etc.);
- (b) Redemption of loyalty points to machine credits;
- (c) Promotional credits awarded; and
- (d) Promotional credits redeemed.

### 7.4.5 Player promotion Account Error Condition

The following conditions must be monitored and displayed to the player:

- (a) Invalid PIN (up to maximum retries allowed);
- (b) Account Locked;
- (c) Abandoned Account;
- (d) Unknown Account/ID;
- (e) Responsible gaming limit(s) reached; and

- (f) A player is no longer receiving loyalty points because they have reached / exceeded their pre-commitment limit.

#### **7.4.6 System Requirements**

1. The CMS must store and report meters and/or significant events for all promotional awards and machine credits play redemption transactions.
2. The player promotion system must maintain the current player promotion account balance.
3. Procedures must be in place to handle “stolen” or “lost” card/account by invalidating the account and transferring all balances into a new account.
4. The player’s current account balance shall be made available on demand at any gaming machine or other system terminals (e.g. loyalty kiosk) after confirmation of the player identity.
5. Any changes to the player promotion scheme must be logged and auditable.
6. Any manual adjustments to the player’s account balance must be logged and auditable.
7. As a minimum the player loyalty system shall be able to provide the following reports:
  - (a) A comprehensive player transaction and account balance report(s);
  - (b) Player promotion account liability report;
  - (c) Promotion configurations; and
  - (d) Promotions reconciliation (i.e. gaming machine bonus meters against promotional transactions / awards).
8. If Random Number Generator (RNG) is used in the player promotion system to determine the award, the RNG must comply with all the requirements specified in relevant sections of this document.
9. The promotion system must be included in the CMS baseline and subjected to CMS software verification and external integrity authentication.

### **7.5 Player bonusing System Requirements**

#### **7.5.1 Database Security**

Bonusing parameters, player bonus awards and transactions must be secure at all times (e.g. prevention of unauthorised access).


#### **7.5.2 Display Notification**

Players shall be suitably notified of all the relevant details on the operation of bonuses. As a minimum, the following shall be provided on the gaming device and/or interface display element:

- (a) Entry and exit from bonusing mode (i.e. Indication of participation in specified bonuses - the availability or unavailability, expiry, etc.);
- (b) Bonus payments awarded; and
- (c) Details on the type of bonus payments awarded.

#### **7.5.3 System Requirements**

1. The CMS must store and report meters and/or significant events for all bonus awards.
2. Any changes to the bonus parameters must be logged and auditable.
3. Any manual adjustments to the bonus payments must be logged and auditable.
4. As a minimum, the player bonusing system shall be able to provide the following reports:
  - (a) A comprehensive detail of all player bonuses awarded;
  - (b) Bonus configurations; and
  - (c) Bonus payment reconciliation (i.e. gaming machine bonus meters against bonus awards).

- 
5. If Random Number Generator (RNG) is used in the bonusing system to determine the award, the RNG must comply with all the requirements specified in relevant sections of this document.
  6. The bonusing system must be included in the CMS baseline and subjected to CMS software verification and external integrity authentication.

## 8 Network and Communication Requirements

### 8.1 Cryptographic Data Security

#### 8.1.1 Introduction

1. Cryptographic data security refers to the protection of critical communication data from eavesdropping and/or illicit alteration (manipulation).
2. Eavesdropping protection is achieved using an encryption algorithm.
3. Protection against illicit alteration is achieved using a message authentication code algorithm although some encryption algorithms also provide this protection.

#### 8.1.2 Requirement for Cryptographic Data Security

Except, as approved on a case by case basis, the following requirements related to cryptographic data security apply:

1. Cryptographic data security must apply to all critical data that traverses data communications lines. This does not apply to communications within a single logic area and
2. Cryptographic data security must apply for all critical data communication transfer between all CMS components located outside the secure computer room, except as approved on a case by case basis.

#### 8.1.3 Encryption Algorithm

The following are encryption characteristics that must be considered:

1. Encryption algorithms must be demonstrably secure against cryptanalytic attacks and must conform to industry standards;
2. The minimum width (size) for encryption keys must conform to industry standard encryption;
3. There must be a secure method implemented for changing the current encryption key set; and
4. 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.

#### 8.1.4 Message Authentication Algorithm

The following are authentication characteristics that must be considered:

1. Message authentication code algorithms are to be demonstrably secure against cryptanalytic attacks;
2. Message authentication code algorithms are to be designed such that it is feasibly impossible to take a hash value and recreate the original message, “impossible” in this context means “cannot be done in any reasonable amount of time.”; and
3. 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.

#### 8.1.5 Encryption Keys

Key algorithms that are used to provide Cryptographic Data Security must conform to industry standard encryption and authentication structures.

## 8.2 Communications Requirements

### 8.2.1 Data Communications Protocol

1. Commission approval must be obtained in advance for any protocol used for gaming related data communications between CMS components.
2. The assessment will also extend to the adequacy of documentation which is to be distributed to selected suppliers for interfacing with the CMS components operating the chosen protocol.
3. The Commission will only approve a protocol if it is confident that the devices implementing the protocol will fully comply with the requirements of this document.
4. The Casino Operator System Equipment must be recoverable to the point of failure following an interruption.

## 8.3 Network Requirements

This section describes the Commission's expected minimum network requirements on system firewalls, network connections that are inside a baseline envelope (the core area agreed by the Commission to be under regulatory control), and network connections from the baseline envelope to external devices.

### 8.3.1 Network Policy Document (NPD)

The Network Policy Document must clearly identify the core areas of the CMS network including but not limited to the network topology of the system, detailing the interconnection of modules within the network, the type of connection between the modules, and the communication protocols that are permitted.

The Licensee must have in place an approved Network Policy Document which details the approved state of the CMS network, what changes must be approved by the Commission and what changes require notification to the Commission.

### 8.3.2 Physical Requirements

1. Power to devices within the baseline envelope must be provided from a filtered, dedicated power circuit. As a minimum standard, this requirement applies to any equipment that is capable of affecting the outcome of a game on a Gaming Machine, a jackpot arrangement, or a significant game play transaction.
2. Cabling used in production networks must be protected against unauthorised physical access and malicious damage.

### 8.3.3 Network Documentation

1. All cabling and devices must be clearly labelled by function.
2. Network documentation must be kept on the primary site and at the disaster recovery site or 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 handling procedures.

### 8.3.4 Connection of External Devices to Networks within a Baseline Envelope

1. Unused ports on network devices and network control devices within the baseline envelope are to be disabled.
2. Configuration changes to all devices within the baseline envelope must be password protected. Password protection policies, procedures and standards must exist and be implemented by the Casino Operator, including provision of prevention, detection and correction measures to address non-compliances.

3. 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 any persons authorised to make configuration changes, and an alert must be produced for all unauthorised changes to an audit log.
4. At a primary site, all network devices, network control devices and hosts associated with a production network must be located inside an area that only authorised persons can access.

### **8.3.5 Communications within a Baseline Envelope**

1. There must be no loss of information due to the failure of a redundant communications network within a baseline envelope.
2. All information traversing the network between remote equipment and the CMS components must be recoverable once communications are restored.

### **8.3.6 Communications between Separate Baseline Envelopes**

1. Critical data 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 Casino Operator.
2. There must be no loss of information due to failure of a redundant communications network between baseline envelopes.
3. Communication between devices in separate baseline envelopes must be immune from “man-in-the-middle” attacks.

### **8.3.7 Communications to Devices outside a Baseline Envelope (Firewall)**

1. Data exchanged with computer systems and terminals outside the baseline envelope must pass through at least one network control device (router or firewall). The network control devices must implement the controls as defined in the Network Policy Document.
2. The network control devices involved in implementing the Network Policy Document must be located within the baseline envelope.
3. An audit log must be maintained for all changes to the configuration of any network control devices within the baseline envelope. The audit trail must not be modifiable by persons authorised to make the configuration changes, and an alert must be produced for all unauthorised changes to an audit log.
4. 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.
5. Computer Systems within the baseline envelope must not be affected by computer/network attacks emanating from outside the baseline envelope (e.g. ping-of-death attacks, teardrop attacks, routing protocol attacks, etc.).
6. Operational procedures for network control devices must include the capturing, regular review and follow-up of all access violations.
7. 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:
  - a) Authentication scheme;
  - b) Physical and logical security of the external terminal devices and computer systems;
  - c) Physical and logical security of the network (including intervening hubs, bridges and routers);
  - d) Connections to the external devices;
  - e) The sensitivity of the information being transferred;
  - f) Whether the computer system inside the baseline envelope or outside the baseline envelope initiates information transfer;

- g) Audit information recorded on the CMS pertaining to the transfer (date, time, person account or system account, and file(s) transferred); and
- h) Intrusion detection mechanism utilised and immunity from man-in-the-middle attacks.

### **8.3.8 Computer Monitoring Systems and Network Management Systems**

1. The configuration of monitoring tools and network management systems must not be installed/changed without formal authorisation consistent with the Casino Operator's access and security procedures.
2. A device outside a baseline envelope must not be able to affect the configuration of network devices or network control devices by any means, including but not limited to:
  - a) Imitating the IP address of a host monitoring system or a network management system;
  - b) Imitating the hardware address (Ethernet address) of a host monitoring system or a network management system; or
  - c) Replaying previously captured communications.
3. A device outside a baseline envelope must not be able to affect the operation of the CMS or be able to read or modify critical data.

### **8.3.9 Verification Tools**

The Commission must, upon request, be provided with sufficient tools and/or procedures to verify the configuration of all devices within the baseline envelope approved by the Commission.



## 9 Submission Requirements

### 9.1 Introduction

The Submission requirements specify the type of information that may be required to be supplied by manufacturers to a gaming machine tester and VCGLR when making submissions for Monitoring System, Jackpot Systems, Table Games, Bonuses & Promotions and related gaming equipment submissions.

### 9.2 New CMS component

#### 9.2.1 General

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

1. Background of the CMS;
2. Purpose of the submission;
3. Description of the scope of system and operational changes;
4. Tester recommendation of the CMS in accordance with above requirements;
5. The Casino Operator's comments on any conditions included in the tester recommendation;
6. List of all software versions and associated SIAs;
7. List of all relevant hardware and operating systems – product names, models and versions;
8. Associated systems that are connected to CMS;
9. A System Document; and
10. A Network Policy Document.

#### 9.2.2 Player information

1. The Casino Operator must provide player registration process details.
2. The Casino Operator must provide descriptions of how player verification information is to be protected from unauthorised access.
3. The Casino Operator must provide details of player authentication.
4. The Casino Operator must provide descriptions of how player registration and account information is to be protected from unauthorised access.

#### 9.2.3 Communications

##### 9.2.3.1 Authentication and Encryption

1. The Casino Operator must provide details of the message authentication algorithm used.
2. The Casino Operator must provide details of the encryption to be used during:
  - a) Encryption algorithms;
  - b) Size of encryption keys;
  - c) Key exchange procedure at session start-up;
  - d) Subsequent key exchanges; and
  - e) Details of any information that is not encrypted for transmission.

##### 9.2.3.2 Internal Network Architecture

1. The Casino Operator must provide details of the proposed architecture of the internal production network to be used to supply CMS facilities:
  - a) Network topology;
  - b) Devices used to create the network; and
  - c) Controls to prevent unauthorised modification to device configuration.
2. The Casino Operator must provide details of any remote connections used (if any) to support CMS operations.

3. The Casino Operator must provide details of authentication and encryption associated with remote connections.
4. The Casino Operator must provide a list of all non-production systems that will connect to the CMS components.
5. For each external system provided in relation to the above section, the Casino Operator must provide:
  - a) The connection method;
  - b) Details of the information to be transferred in each direction;
  - c) The entity that initiates the information transfer;
  - d) The protocol used to perform the transfer;
  - e) The controls in place to prevent unauthorised access to other information;
  - f) The controls in place to prevent unauthorised use of the connection; and
  - g) The controls in place to prevent eavesdropping on communications between non-production systems and the CMS components.
6. The Casino Operator 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 Casino Operator) to the internal production network.
7. The Casino Operator must provide details of controls and audit trails associated with access and modifications to network components.
8. The Casino Operator must provide details of any network management system associated with the internal production network, including:
  - a) The physical location of the network management system;
  - b) The class of personnel authorised to use the network management system;
  - c) The locations from where network management functions can be executed;
  - d) The network management protocol;
  - e) The devices to be managed on a read only basis;
  - f) The devices to be managed on a read/write basis;
  - g) The controls in place to prevent unauthorised access to network management functions;
  - h) The controls in place to audit the use of network management functions;
  - i) The controls in place to detect unauthorised connections to the network; and
  - j) The controls in place to detect connection of unauthorised equipment to the network.

#### 9.2.3.3 Third party connections

1. The Casino Operator must provide a list of all third-party systems that will connect to the CMS components.
2. For each external third-party system provided in relation to the above section, the Casino Operator must provide:
  - a) The connection method;
  - b) Details of the information to be transferred in each direction;
  - c) The entity that initiates the information transfer;
  - d) The protocol used to perform the transfer;
  - e) The controls in place to prevent unauthorised access to other information;
  - f) The controls in place to prevent unauthorised use of the connection; and
  - g) The controls in place to prevent eavesdropping on communications between Third Party connections and the CMS components.

#### 9.2.4 CMS Infrastructure

1. The Casino Operator must provide an overview of the CMS design.
2. The Casino Operator must provide a functional specification of the CMS.
3. The Casino Operator must provide detailed CMS design documents.
4. The Casino Operator must provide details of all computer systems used by the CMS including, but not limited to:
  - a) Hardware platform;
  - b) Operating system;

- c) Applications;
  - d) Audit subsystem;
  - e) Duplication strategy;
  - f) Disk subsystem;
  - g) Back-up facilities;
  - h) Physical security;
  - i) Login security;
  - j) Power requirements; and
  - k) Environmental condition requirements.
5. The information requested in relation to the above section also applies to all other CMS equipment to be used in the CMS computer environment.
  6. The Casino Operator must provide descriptions of where and how information is stored throughout the system.
  7. The Casino Operator must provide detailed descriptions of its password protection systems and associated algorithms utilised by the system.
  8. The Casino Operator must provide a description of the method of transaction logging used.
  9. The Casino Operator must provide details of situations during which encryption of data files will be employed.
  10. The Casino Operator must provide a description on how self-monitoring is to be implemented.

## **9.2.5 CMS software**

### **9.2.5.1 Open Source Code**

For all open-source software, as a minimum the following shall be provided:

1. Source code files;
2. Make or batch files;
3. Map files;
4. Master images; and
5. Any other files used in conjunction with the master images.

### **9.2.5.2 Closed Source Code**

For all closed-source software, as a minimum the following shall be provided:

1. Master images from the closed-source development environment, and
2. Any other files used in conjunction with the master images.

VCGLR may also require that arrangements with the closed-source software vendor are in place to allow appropriate access to the source code by the regulator and/or the tester for the purpose of investigating software faults.

### **9.2.5.3 Compilation Environment**

1. The Casino Operator and/or suppliers of the CMS must make available to the Commission or an Accredited Testing Facility source code for all the baseline components.
2. The necessary development environment, or access to that environment where software development facilities differ from those available within the evaluation laboratory.
3. User guides, programming guides, instructions and/or manuals necessary to create the software.
4. The output of the compilation or build process must be reproducible on subsequent Build. Where the output of the compilation or build process is entirely reproducible on subsequent builds, the output must be able to be verified against the master images provided in the software submission.

5. Where the output of the compilation or build process is not entirely reproducible on subsequent builds:
  - a) The build environment, build process and all inputs must be fully documented and verified by the tester;
  - b) The subject of the evaluation by the tester must be the software resulting from the successful verification at (a);
  - c) The software deployed to production must be the software resulting from the successful verification at (a); and
  - d) All software components that will change if the build is repeated must be identified by the manufacturer.
6. If any special software or hardware tools need to be used by the tester to verify software due to copy or intellectual property protection, these tools must be supplied free of charge by the manufacturer. If they are not available, then the manufacturer must develop and supply them to the gaming machine tester free of charge.
7. All software and manuals provided must be legal and licensed copies.
8. The Casino Operator must provide a description of the method to be used to verify the integrity of the software operating on the production CMS.
9. The Casino Operator and/or suppliers of the CMS must provide commission or an authorised tester copies of operator's manuals, operator's procedures manuals and system administrator manuals or equivalent.

### 9.2.6 Random Number Generator

As a minimum, the following information shall be provided:

1. Full details in technical terms of random number and symbol selection/mapping.
2. All text and journal references used in the design of the RNG. Provision of this information may assist in reducing testing costs and the evaluation time.
3. All points in game play and the gaming program operation where the RNG is activated, updated, or numbers are obtained, including details of background RNG activity.
4. Explain the seeding process of the RNG.
5. A detailed flow chart and software listing of the RNG process.
6. Results for any empirical and/or theoretical tests conducted on the RNG.

## 9.3 Updated CMS component

### 9.3.1 General

The submission to update an approved CMS component for Commission approval, at a minimum, must include the following:

1. Purpose of the submission;
2. Description of the scope of system changes and operational changes;
3. Tester recommendation of the CMS in accordance with the above requirements;
4. Casino Operator's comments on any conditions included in the tester's recommendation;
5. List of all software versions and associated SIAs;
6. List of all relevant hardware and operating systems – product names, models and versions;
7. Updated System Document; and
8. Updated Network Policy Document (NPD).

## 10 Other CMS Requirements

### 10.1 Approval and Notification Requirements

Any changes to the CMS components that have been defined by the Licensee to be within the baseline envelope must have Commission approval before being activated.

Commission approval is not required for the components outside the baseline envelope (non-baselined components), however the Licensee must notify the Commission within 14 days of installing a new First Tier non- baseline component on the CMS.

To ensure the VCGLR has visibility to the complete CMS, the Licensee must maintain and submit, on an annual basis, a complete CMS document outlining:

1. Network topology of the complete end to end CMS and communication infrastructure;
2. All baseline components;
3. All first and second tier non-baseline components;
4. Any changes implemented in the last 12 months, or in comparison to the last CMS document; and
5. The method and mechanisms used to verify that the CMS is operating in an approved state;

The CMS document must be regularly maintained and made available to the VCGLR upon request.

### 10.2 Storage Area Policy Document (SAPD)

This document details the configuration of the storage area network topology. The Licensee must have in place an approved Storage Area Policy Document.

### 10.3 Audit, Verification and Control

The Licensee shall maintain methods and procedures to ensure the security and integrity of the CMS components, including but not limited to, processes and procedures that ensure:

1. A method to verify the integrity of all baseline components listed in the CMS document;
2. All changes to the baseline components must be authorised by the Commission before they are implemented;
3. CMS shall have software change control procedures and the Licensee must maintain audit logs for the changes;
4. The Licensee shall ensure that components of the system(s) outside the baseline are checked regularly to ensure that unauthorised activities are not taking place on the CMS; and
5. Baseline components shall be version controlled or labelled and contain sufficient information to identify any modification.

### 10.4 Cloud Computing

Refer to the VCGLR Regulatory Framework and Application process for requirements on cloud computing.

## 11 Glossery of Terms

Term or Abbreviation	Description
<b>Act</b>	The Casino Control Act 1991 (Vic), as amended from time to time.
<b>Agreement</b>	Any related agreement entered into between the Minister and the Licensee in accordance with Part 2 of the Act.
<b>Baseline</b>	The term baseline refers to all components that are defined as core to the CMS by the Licensee and approved by the Commission at a point in time, that thereafter serves as the basis for defining incremental changes to the CMS.
<b>Baseline Envelope</b>	This term refers to an envelope around a CMS over which the Commission maintains verification control.
<b>Casino Operator</b>	Means a person who is the holder of a licence granted under Part 2 of the Act.
<b>CMS</b>	The Central Monitoring System (CMS) consists of any component (hardware or software) that enable the CMS to operate in a secure environment and meet the legislative requirements and the licensee's obligations under the relevant License they hold.
<b>Commission</b>	The Victorian Commission for Gambling and Liquor Regulation established under the Victorian Commission for Gambling and Liquor Regulation Act 2011, or any successor body.
<b>Critical Memory</b>	Memory locations storing information that is considered vital for the continued proper operation of the CMS.
<b>Gaming Equipment</b>	Has the same meaning as defined in the Act.
<b>EGM</b>	Electronic Gaming Machine – has the same meaning as provided in the Gaming Machine National Standards.
<b>Electrostatic Discharge (ESD)</b>	The sudden and momentary electric current that flows between two objects at different electrical potential that may cause damage to electronic equipment.
<b>EMI</b>	Electro Magnetic Interference - the physical characteristic of an electronic device to emit electronic noise either into free air, onto the mains power lines, or communication cables.
<b>Firewall</b>	Part of a computer system or network that is designed to block unauthorised access while permitting authorised communications.
<b>Firmware</b>	The layer of fixed programs and data structures between the software and hardware that internally controls the hardware and electronic devices.
<b>Licence</b>	Means a licence granted under Part 2 of the Act.
<b>Memory</b>	An area of a computing device used to store data and/or instructions.
<b>Minister</b>	The Minister for Gaming for the State.
<b>Australian/New Zealand Gaming Machine National Standards</b>	The core requirements, common to all jurisdictions, for the design of Gaming Machines and games for operation throughout Australia and New Zealand and to guide testers in their testing for compliance with the standard.
<b>PID</b>	Player Information Display.
<b>PIN</b>	Personal Identification Number.
<b>Pre-Commitment</b>	A mechanism to allow players to stay in control of their gambling and make informed decisions about their play.
<b>Protocol</b>	The means for communication between the gaming devices and CMS.
<b>PSD</b>	Program Storage Device.
<b>RFI</b>	Radio Frequency Interference - the ability to influence an electronic device by means of using radio waves.

<b>RNG</b>	Random Number Generator - a method of producing a sequence of random numbers.
<b>Roll of Manufacturers, Suppliers and Testers</b>	Has the same meaning as defined in the Gambling Regulation Act 2003.
<b>RTP</b>	Return to Players - The ratio of total wins (including progressives and other features) to the total turnover in a Game cycle (note: gamble bets do not affect turnover and total wins is only affected by the final gamble outcome).
<b>SIA</b>	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.
<b>Tester</b>	A tester listed on the Roll of Manufacturers, Suppliers and Testers as defined in the Gambling Regulation Act 2003.
<b>UPS</b>	Uninterruptible Power Supply (a no-break mains power supply including battery backup equipment).
<b>VCGLR</b>	Victorian Commission for Gambling and Liquor Regulation
<b>Verification Control</b>	Verification Control is a means of confirming that the component used in production is equivalent to that approved by the VCGLR.
<b>Version Control</b>	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".
<b>Victoria</b>	The State of Victoria.