Victorian Commission for Gambling and Liquor Regulation

Technical Requirements for
Central Monitoring System
in the Melbourne Casino

The "Technical Requirements Document"

Version 4.05

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).

Table of Contents

1 INTRODUCTION

1.1 General Information

1. This Central Monitoring System requirements document (CMS) contains the system related requirements for the Monitoring System, Jackpot Systems, Electronic Table Games, Bonuses & Promotions and related submissions for operation in the Crown Casino in Melbourne.
2. The Requirements specified in this document are supplementary and do not take the place of any of 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. The Electronic Gaming Machine and games shall comply with the current version of the Commission 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 proport 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 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 EGM MONITORING AND CONTROL

2.1 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:
    a. Unique identification number (Serial Number or Asset Number)
    b. Unique Floor location number;
    c. Status of the game;
    d. Manufacturer Name;
    e. Game type such as single game, multigame, ante-bet game etc.;
    f. For each game provide the following:
        1. Game Name;
        2. Maximum Bet;
        3. Denomination of the game;
        4. Jackpots and promotions configured for the game; and
        5. Theoretical hold of the game with & without jackpot contributions;
    g. Base/Shell/OS program identifiers;
    h. Game program identifiers;
    i. Accounting meters (as specified in Commission Standards);
    j. Peripheral configurations; and
    k. Functionality supported such as Ticket In/Ticket Out, Cashless, etc.
4. The CMS shall be capable of reading each gaming machine configuration directly from the gaming machine by using its unique id;
5. The CMS shall be capable of reading each individual gaming machine meters directly from the gaming machine;
6. The CMS shall maintain a complete history of changes made to the configuration of all gaming machines;
7. The CMS shall maintain a complete history of changes made to the configuration for a given floor location;
8. The CMS shall have the capability to print and/or display all the retained historical information based on the unique identifying fields;
9. The CMS shall be capable of designating which gaming machines offer jackpots;

10. The CMS shall provide the capability to account for standalone jackpot configurations;
11. All information relating to jackpot/progressive configuration and winnings shall be maintained in the CMS;
12. The CMS shall support the capability of issuing real time commands to the gaming machine for information retrieval and gaming machine control functions;
13. The CMS shall store the history of all machine events. 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.)
14. The date and time displayed by the CMS shall meet the Australian format; and
15. The CMS shall provide the capability to easily attach/detach gaming machines with jackpot configurations to/from the jackpot system.

2.2 Game Verification

1. Game verification shall be automatically triggered for specific event(s) or initiated by a user command from the CMS or from the EGM. To ensure full coverage, gaming verification should be performed after each of following incidents:
   a. EGM power up;
   b. Establishment of communication to the CMS;
   c. Game win over a specified amount; and
   d. Loading of the program files.
2. The CMS shall be notified (through an exception triggered by the EGM) when a signature verification check failure occurs on any EGM.
3. When a signature check failure is recognized, the failed EGM shall be prevented from performing any monetary transaction.

2.3 Metering

1. The CMS shall be able to collect and individually report all the meters specified in the Commission Standards.
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.
4. At a minimum, the CMS shall collect and store all the meters specified in the Commission Standards 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 decimal places.

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 at any point of time 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 received a suspect meter value from 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.

2.4 Exception Reporting

1. The CMS shall have the capability to store and report all the events specified in the Commission Standards.

2. 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.

3. The CMS shall report any loss of communication to any gaming machine or to any other nodes. It shall also report when communications are re-established.

4. The CMS shall report 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 applicable exception reporting shall also be stamped with the user name and employee identification.

2.5 Functionality

1. The CMS shall include capability to capture and process every handpay message from each gaming machine. A method by the CMS to provide the player/attendant with a unique transaction number for each handpay 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 authorized user.
3. Once captured, there must be access controls to allow for authorization, alteration, or void of any values prior to payment.

2.6 System requirements

2.6.1 Server

1. The CMS shall comprise of networked systems that direct overall operation and an associated database that stores all entered and collected information.
2. The CMS shall be designed so that no single point failure of any system component will cause the cessation of the system operation.

2.6.2 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 must 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 shall 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 the primary 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 the Commission Standards.

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.

2.7 Security requirements

2.7.1 System Requirements

1. The architecture of the CMS shall be designed such that under normal operating conditions no single point of failure would interrupt the operation of the CMS.
2. The computer rooms of the central computers of the CMS shall meet the relevant Australian National Standards 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 computerized 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 unauthorized 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 wireless interfaces.

16. All successful and unsuccessful access attempts to CMS hosts shall be recorded in an audit trail.

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 automated audit log must be generated at a minimum to capture 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.

21. The system(s) used for developing or testing shall be completely separated from the live system and its database.

22. If the CMS supports remote access, the procedures for this access shall be approved by the VCGLR.

23. Firewalls and/or any other industry acceptable methods must be utilized to protect against unauthorized access.

24. 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.

25. A program must be available that will list all registered users on the system including their privilege level.

26. CMS items (e.g. servers, gateways, communication controllers etc) located in any area not restricted to authorized personnel shall be securely housed, physically locked and shall have door open sensors.

2.7.2 CMS Recovery

2.7.2.1 Host CMS Recovery

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

2.7.2.2 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) all transactions received from all Gaming Equipment, Jackpot systems, table game systems, cashier stations, control stations, cash counters and other elements 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 serially 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.

2.7.2.3 Format of Log Records

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

d. Any relevant data that is associated with the event; and

e. A unique event identifier 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.

2.7.2.4 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, that is approved by the Commission, and conduct disaster recovery testing in accordance with the approved plan.

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

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.

2.7.2.5 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.

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

3. Some typical tests that may be implemented by the Commission or its representatives to test compliance are:

   a. Failure of central processor;

   b. Failure of central computer power supply;

c. Failure of central computer Memory;

d. Failure of central computer disk(s);

e. Failure of central computer I/O channels;

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

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

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

2.7.3 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 three (3) 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.

2.7.4 Duplication

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

2.7.5 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.

2.7.6 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.

2.7.7 Code Download Requirements

1. Downloads or uploads of code from or to CMS hosts shall be secure using industry best practices and shall be approved by VCGLR.
2. An audit log shall record the time and date of any download. The audit log shall also contain which version(s) of code was downloaded and the user who initiated the download.

2.7.8 System Integrity

1. The CMS system shall have the capability to automatically authenticate the identity of all the devices that are connected to the CMS. This authentication shall be performed at least after each of the following events:
    a. Before they are first enrolled on the system;
    b. Establishment of communication to the CMS;
    c. When initiated by an authorized user; and
    d. 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. Any communication received from any nodes not authenticated by the CMS shall be reported in the exception reporting.
5. The CMS shall have the capability to detect and record any unreasonable or corrupt communication information received.
6. The CMS shall have the capability to periodically authenticate the various nodes within the system.
7. The CMS shall have the capability to manually verify the authenticity of a given node at any time using a selected seed.
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.

2.7.9 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 sixty (60) days of data. 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;

    a. Identity of the EGM/node that generated the event;

    b. A unique number that defines the event; and

    c. A brief text that describes the event.

3. In the event of an unauthorized 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. Such error conditions shall be rectified within the time frame stipulated by the 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).

5. The CMS shall detect and alert any unauthorized changing of the events log and/or game play transactions.

2.7.10 CMS Components, Documentation and Verification

System Components

The Central Monitoring System (CMS) consists of any instrument, contrivance, computer hardware or software that the Licensee proposes to use that enable the system(s) to operate in a secure environment and meet the legislative requirements.

The Commission recognises that not all systems operated by the Licensee are for the purposes of gambling within the Casino. As such it is critical to identify all components of the system(s) and identify their attributes. Together with the assistance of the tester, the Licensee and the Commission will identify the components of the system(s). These can be grouped into following core categories –

1. **Baseline Components**
   All software, hardware and any other components that enable the system(s) to operate in a secure environment and meet the legislative requirements.

2. **First Tier Non-Baseline Components**
   Interface devices/modules/third party services and related software (non-baseline) that are directly interacting with baseline system(s) components.

3. **Second Tier Non-Baseline Components**
   Interface devices/modules/third party services and related software (non-baseline) that are not directly interacting but may nevertheless have impact to the baseline system(s) components.

4. **Third Tier Non-Baseline Components**
   Interface devices/modules/third party services and related software (non-baseline) that are not directly interacting and do not have any impact to the baseline system(s) components.

Note

Any modifications, additions or deletions to the system(s) components must be formally reviewed and identified as one of the abovementioned categories by the Licensee, and agreed by the Commission, prior to implementation.

Baseline

The term baseline refers to all components that are defined core (baseline component) to the system(s) 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 overall system(s).

Any modifications, additions or deletions to the baseline must be approved by the Commission prior to implementation.

System Document

This document shall be developed covering the following core areas, including, but not limited to –

1. Baseline Components.
2. First Tier Non-Baseline Components.
3. Second Tier Non-Baseline Components.
4. Logical Overview of the network connectivity.
5. Identification of any operations or procedures relevant to securing and controlling the system(s).
6. Identification of any other special operational or procedural issue that is relevant to the Commission.

This document shall be prepared by the Licensee and approved by the Commission.

Note

The licensee may choose to supply the System Document with or without 3rd tier components.

CMS Audit, Verification and Control

The operator shall maintain methods and procedures to ensure the confidentiality, integrity and authenticity of the CMS components -

1. The CMS shall provide a method to verify the integrity of all baseline components listed in the System Document.
2. All changes to the baseline components listed in the System Document shall be authorized by VCGLR before they are implemented.
3. All CMS hosts shall have software change control procedures and the operator must maintain a log of changes to the infrastructure.
4. There shall be adequate procedures in place to ensure that portions of the system(s) outside the baseline envelope are checked regularly to ensure that unauthorized activities are not taking place on the system.

5. Software (e.g. individual application files) shall be clearly labelled and contain sufficient information to identify the version and any modification.

It is necessary for VCGLR to maintain visibility of all components of the System. The licensee shall provide the following to VCGLR on an annual basis –

- System Document.
- Consolidated non-baseline notifications for incremental changes.

2.7.11 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. All critical data communication shall be protocol based and incorporate an error detection and correction scheme to ensure an accuracy of ninety-nine (99%) or better of message received;
    b. The defined communication protocol shall include the following:
        i) Error Control;
        ii) Flow Control; and
        iii) Link Control (remote connection).
4. In event of communication breakdown between the EGM and 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.

2.8 Reporting Requirements

1. The CMS shall have the capability to generate all the financial reconciliation and variance reports as specified by VCGLR.
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 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 user name and employee identification or similar identifier in the reports. For systems that do not provide this capability, the casino must maintain controls to ensure all reports include the operating user name or similar identifier.

14. All reports shall include the casino name.

2.9 Voucher In/voucher OUT

2.9.1 General

A ticket/voucher validation system may be entirely integrated into a CMS or exist as an entirely separate entity. A gaming machine 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 (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.

2.9.2 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 authorized casino staff; and
5. Jackpot hand pay tickets by an authorized casino staff.

2.9.3 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 voucher validation system.
3. The validation system shall process voucher redemptions correctly according to the secure communication protocol implemented.
4. The Ticket/Voucher host shall have the capability to validate and accept only genuine and authorized vouchers. This validation technique shall have as a minimum, the capability to prevent validation of duplicate, incomplete, voided, reproduced or copied vouchers.
5. The Ticket/Voucher system shall provide the capability for the display of relevant informative messages whenever a player-initiated ticket or voucher is being processed for payment.
6. The Ticket/Voucher system shall have the capability to limit accepting of tickets only up to the value approved by VCGLR.

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. Voucher status;

   c. Voucher value; and

   d. Machine number or source identification from where the voucher information came from.

8. The validation system shall be able to identify and notify the cashier of the following conditions:

   a. Voucher cannot be found on file (stale date, forgery, etc);

   b. Voucher has already been paid;

   c. Amount of voucher differs from amount from file (if supported); or

   d. The voucher is in an intermediate/lockup state

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

2.9.4 Ticket/Voucher Issuance

1. The Ticket/Voucher system shall guarantee the authenticity of any voucher generated by the system.

2. The Ticket/Voucher system shall provide the capability for the display of relevant informative messages whenever a player-initiated ticket or voucher issuance is being processed.

3. Validation number to be printed on a voucher will be generated by the validation system.

4. The algorithm or method used by the validation system to generate the voucher validation number shall guarantee uniqueness and non-repetition.

5. The validation system shall only accept one (1) authorized voucher per valid validation number.

6. The Ticket/Voucher system shall have the capability to limit printing of tickets only up to the value approved by VCGLR.

7. The validation system shall record the voucher information correctly and store the voucher information into the database.

8. The Ticket/Voucher system shall record all the details associated with vouchers generated by any gaming machines. Recommended fields to be included in a voucher are given below:

   a. Casino/Establishment name;

   b. Gaming machine number;

   c. Gaming machine unique floor location;

   d. Date & time of voucher issuance in local time;

   e. Amount in numeric format as well as in words;

   f. Sequence number;

g. Validation number;

h. Date printed;

i. Type of voucher being generated (cancel credit, jackpot payment, promotional voucher etc.); and

j. 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 voucher (eg: Pending, Void, Paid, Un-paid, Locked)

10. In the event communications between the system and a gaming device is lost, the Ticket/Voucher system shall allow no more than one voucher to be printed.

11. The voucher shall be printed on secure stock.

12. Any capability to generate off line ticket/voucher printing (if supported) shall be approved by VCGLR.

2.9.5 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 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 automated 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 vouchers issued by a gaming machine, as approved by the VCGLR. Vouchers 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 voucher information or in the generation of duplicate vouchers.

7. The Ticket/Voucher system shall have the capability to generate daily monitoring logs of user accesses, security incidents and unusual transactions.

8. The Ticket/Voucher system shall have the capability to generate a report on all redeemed vouchers.
9. The Ticket/Voucher system shall have the capability to generate a report of all printed vouchers.
10. The Ticket/Voucher system shall have the capability to generate a report of all expired vouchers.
11. The Ticket/Voucher system shall have the capability to generate a 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 if it does not contradict the requirements specified in this Standard.

2.10 Cashless systems

2.10.1 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 for identifying the player, then the same cards 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'*.

2.10.2 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. Digital identification methods such as QR codes; or
5. Biometric identification techniques.

2.10.3 Types of Players

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

2.10.3.1 Registered Players

1. The casino shall register a player as a registered player only if the casino 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. Multiple registered identification methods are not permissible for the same person.

3. If a registered player is inactive for more than a time specified by VCGLR, the funds are considered to be unclaimed and the casino shall comply with the '*Unclaimed Money Act 2008*'.

4. The player must set a pin at the time of issuing the identification device.

2.10.3.2 Anonymous or Casual Player

1. Instead of a registered player, a player may request, and the casino 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.

3. If an anonymous or casual player is inactive for more than a time specified by VCGLR, the funds are considered to be unclaimed and the casino shall comply with the '*Unclaimed Money Act 2008*'.

4. The casino 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.

2.10.4 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 authorized 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 be able to select the amount to be transferred from their player account or the entire balance on the card to the EGM. This amount cannot override any regulatory limits.

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 unauthorized 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 for a time specified by VCGLR 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) as approved by VCGLR. 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 approved by VCGLR.

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

2.10.5 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 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 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.
4. The cashless 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 cashless system shall be designed to ensure that a power loss or a restart of any node will not result in incorrect account balance.
6. The cashless system shall have the capability to generate daily monitoring logs of user accesses, security incidents and unusual transactions.
7. The cashless system shall have the capability to generate a report of all 'funds in' and/or 'funds out' for a given period.
8. 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.
9. The cashless system shall have the capability to generate a report of all expired player accounts.
10. The cashless system shall have the capability to generate a cashless liability report.
11. The cashless system shall produce an audit trail message for every user login and logouts.
12. The cashless system shall ensure that no duplicate funds transfer in or out will be generated by the system.
13. The cashless system shall also comply with any requirements specified by the casino if it does not contradict the requirements specified in this Standard.
14. The cashless system shall have a facility to stop all gaming activities for a player when a suspect transaction has occurred. Additionally, there shall be approved procedures to commit or roll back any suspect transactions.
15. The cashless system shall have a capability to produce a report on all commit and/or roll back transactions performed for a given period.

16. As a minimum, the player authentication data (e.g. Pin) must be encrypted in a non-reversible form for storage and use.
17. The cashless system must keep separate meters for different types of credits supported by the system such as cashable credit, non-cashable credit, promotional credit etc.
18. If cashable, non-cashable and promotional credits are combined to a single credit meter at the gaming machine, the cashless system shall apply all promotional credits followed by non-cashable credits to a player's wagering activity before applying any cashable credits.

2.10.6 Reportable Events

The cashless system 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);
7. When a player attempts to access an account with incorrect authentication details;
8. When a player's account is locked;
9. When a player's account is locked by the system;
10. When a casino performs a commit/Rollback transaction including the details of the transaction; and
11. The cashless system shall provide an online search facility that enables comprehensive searching of the event log for all pending, completed and failed 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 Time range;

    b. Unique gaming machine/kiosk/Cashier's desk identification number; and

    c. Patron's wagering/promotional account information.

2.10.7 Display Requirements

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

1. The type of transaction (Credit transfer In, Cashable/Non-Cashable Electronic Promotion In or Credit transfer Out, Cashable/Non-Cashable Electronic Promotion Out);
2. The transaction value;
3. The time and date; and
4. A descriptive message on the success or failure on the transaction initiated.

A message describing the type of error shall be displayed to the patron at the player interface module in the event of the following error conditions:

1. Invalid PIN (can prompt for re-entry up to maximum allowed);
2. If a player initiates a cashless transaction and that transaction would exceed the maximum permissible EGM credit limit;
3. Where a transaction will result in exceeding the maximum permissible credit limit on the player's account; and
4. Any conditions, such as expiration of promotional credit, shall also be made known to the player.

2.11 Cash Redemption Terminals (CRT)

2.11.1 Purpose

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

2.11.2 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 for unpaid amounts;
5. View responsible gaming parameters;
6. Convert player points to credits; and
7. Dispense funds for other payments such as jackpot payouts.

2.11.3 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 unauthorized 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 unauthorized 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 Electro Static Interference specifications given in the Commission Standards.
9. The coin acceptor, diverter and the bill acceptor used in the CRT shall comply with the specifications given for these components in the Commission Standards.
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.

2.11.4 Software Requirements

1. CRTs must only perform authorized, correct and legitimate transactions when dispensing cash, accepting tickets, dispensing funds for manual payments or transferring funds to/from player cashless account. All these transactions at the CRT must be authorized 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 using a cryptographic hash algorithm as specified in the Commission Standards.
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 for redemption at a Cashier only. These receipts must not be able to be inserted into TITO systems and used for credits.
12. Short pay receipts issued by CRTs must clearly display “Short Pay Receipt” and “Please see Cashier” and contain the following information: terminal identification, venue name, date and time receipt was generated, amount paid, amount owing and a reference or authentication code unique to the transaction
13. 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.
14. The CRT must perform a self-check of all executables at least on every power up. It is desirable to 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.
15. 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.

2.11.5 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 following Gambling Helpline contact details:

   "*Gambling too much? For free and confidential advice 24/7 call the Gambling Helpline on 1800 858 858 or visit gamblinghelponline.org.au*".
6. Artwork must not promote the consumption of alcohol while gambling.

3 JACKPOTS

This section covers the requirements for operation of jackpots on Electronic Gaming Machines

3.1 Jackpot Types

3.1.1 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.

3.1.2 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.

3.1.3 Standalone Progressive Jackpot

If a jackpot is only winnable on a single gaming machine, it is considered a SAP.

3.1.4 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.

3.1.5 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.

3.1.6 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.

3.1.7 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.

3.1.8 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.

3.1.9 External Jackpot system

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

3.1.10 Internal Jackpot system

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

3.1.11 Communication Failure

A gaming machine shall disable itself within at least 3 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 3 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.

3.2 Mystery Jackpots

3.2.1 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 a procedure approved by VCGLR. 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 75% of the maximum pool value when added with the other pools such as hidden pool, off line pool, overflow pool etc.

3.2.2 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 generate an event when an unreasonable meter event is detected. This event as a minimum shall have the following information:
   a. Amount of contribution received;
   b. The identification of the gaming machine that generated the event;
   c. Jackpot identification; 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 will disable the affected gaming machines. The disabled gaming machines shall display an appropriate error message. The “unreasonable contribution” amount shall be set up based on the maximum possible bet for the relevant pool.
3. Crown shall submit the procedure for enabling EGMs disabled by a jackpot controller due to an unreasonable jackpot contribution to the VCGLR.

3.2.3 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 the Random Number Generator section of The Commission Standards.
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 possible to win a jackpot while playing in this EGM.

3.2.4 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'.

3.2.5 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.

3.2.6 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.

3.2.7 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 automatically produce a report which shall contain as a minimum the following:
    a. Date of Parameter Change;
    b. VCGLR approval details for the change;
    c. Person authorizing the change;
    d. Person making the change;
    e. Parameter values before the modification; and
    f. Parameter values after the modification.

3.3 Progressive Jackpots

3.3.1 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. off line pool, overflow pool) must be dispersed according to a procedure approved by VCGLR.
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 upto 14 decimal points, for the same denomination played.

3.3.2 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. This event as a minimum shall have the following information:
    a. Amount of contribution received;
    b. The identification of gaming machine that generated the event;
    c. Jackpot identification; 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 will disable the affected gaming machines. The disabled gaming machines in the group shall 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. Crown shall submit the procedure for enabling the EGMs after it has been disabled by a jackpot controller due to an unreasonable jackpot contribution to VCGLR.

3.3.3 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. Crown is required to submit a procedure for handling simultaneous wins for VCGLR approval. 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.

3.3.4 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.

Crown is required to submit a procedure for handling jackpot wins when communication to the jackpot controller is lost for VCGLR approval.

3.3.5 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.

3.3.6 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 automatically produce a report which shall contain as a minimum the following:
    a. Date of parameter change;
    b. VCGLR approval details for the change;
    c. Person authorizing the change;
    d. Person making the change;
    e. Parameter values before the modification; and
    f. Parameter values after the modification.

3.4 JACKPOT CONTROLLER REQUIREMENTS

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

3.4.1 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.

3.4.2 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 authorized accessibility.
2. Provision must be made for a physical seal on the logic area door which must be broken on entrance or removal of the logic area.
3. The jackpot controller shall comply with the applicable requirements specified in the Commission Standards.

3.4.3 Critical Memory

1. Jackpot controller critical memory shall be implemented as specified in the Commission Standards.
2. All jackpot controller parameters and meters shall be stored in the critical memory.

3.4.4 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.

3.4.5 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. Overglow 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;

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.

3.4.6 Error Conditions

1. When a jackpot controller error occurs, an appropriate error message and the current jackpot prize pool shall be made visible to all the players affected by the error, and the casino shall be alerted of the error condition.

2. If any of the following events occur, the jackpot controller shall convey the appropriate signal to disable all the gaming machines in the jackpot group, and an error shall be displayed on the jackpot display and all the gaming machines in the group:

   a. When a jackpot controller signature check has failed;

   b. When a jackpot controller's unrecoverable critical memory failure occurs or a PSD (program storage device) mismatch is detected;

   c. When the jackpot configuration is lost or not set; or

   d. If supported, the game meters recorded by the CMS are validated against the game meters recorded by the jackpot controller and they do not reconcile (not applicable for internal jackpot systems).

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.

3.4.7 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.

3.4.8 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. Jackpot system control programs shall test themselves for possible corruption due to failure of the program storage media using a robust and proven mechanism; and
   c. The integrity of all critical memory shall be checked.

3.4.9 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.

3.4.10 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'

3.4.11 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 the Signature Verification section of the Commission Standards or better.

3.4.12 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.
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 must 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.

3.4.13 Jackpot Win

3.4.13.1 Jackpot Win Notification

1. The following indications for the winning of a jackpot prize are required:
   a. Audible;
   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 from which the jackpot was paid;
   c. Date & time; and
   d. Method of payment (Paid to the credit meter or handpay 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.

3.4.13.2 Winning Gaming Machine

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

a. Display the winning prize;
b. 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
c. All jackpot related meters shall be updated to reflect the winning jackpot amount.

3.4.13.3 Reset of Jackpot Amount

1. The jackpot controller shall have the ability to reset the current jackpot amount to the start up 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 Crown’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.

3.4.14 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.

3.4.15 Reporting Requirements

The jackpot controller shall be capable of generating all the reports required by VCGLR. 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.

3.4.16 Time Synchronization

3. 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.
4. The jackpot controller shall support capability to synchronizing time with an external reference clock.

3.5 Tournament Jackpots

3.5.1 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.

3.5.2 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.

3.5.3 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.

3.6 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 no later than 10 seconds 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. How many jackpots will be awarded for a single jackpot trigger; and the rule for each prize determination;
    b. The individual maximum value of any jackpot that can be won;
    c. The rule for sharing the jackpot prize between the participating EGMs; and
    d. A statement that an EGM not played up to 10 seconds 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.

3.7 Communications

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

3.7.1 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.

3.7.2 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.

4 ELECTRONIC TABLE GAME REQUIREMENTS

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

1. A Semi-Automated Table Games (SATG) that requires a live dealer for the determination of the game outcome. The terminals are used to determine the game payouts based on the individual bet & game result, as a means for entering and collecting credits and sending all communication packets to the host as specified in the protocol supported by the CMS.

2. A Fully Automated Electronic Table Games (FATG) is where a central server will be used to determine the game results. The terminals are used to determine the game payouts based on the individual bet & game result, as a means for entering and collecting credits and sending all communication packets to the host as specified in the protocol supported by the CMS.

4.1 Common Requirements

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

4.1.1 Applicability of EGM Technical Standards

SATGs and FATGs shall comply with the requirements stipulated in the Commission Standards 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.

4.1.2 Game Rule

1. All game rules and payout must not deviate from the corresponding official game rules approved by VCGLR;
2. The video display used to communicate game play information 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 paytable information must 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, seated at a player interface terminal to which the game is connected; 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.

4.1.3 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).

4.1.4 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.

4.1.5 Player Interface Terminal Requirements

The player interface terminal(s) must comply with all the relevant hardware and software requirements specified in the current version of the Commission Standards.

4.1.6 Player Interface Error Circumstances

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

4.1.7 Game Recall

4.1.7.1 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.

4.1.7.2 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 Commission Standards) 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.

4.1.8 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.

4.1.9 Artwork

1. There must be sufficient information to allow a player to determine the correctness of prizes awarded.
2. The paytable 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 shall be in English unless specifically approved by the Commission and all messages displayed shall be both grammatically and syntactically sound, in the languages. 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.

4.1.10 Significant Logs and Events

Significant events produced by the terminal shall be sent directly to the CMS utilizing a Communication Protocol supported by the CMS.

All significant events that occur at each terminal will be monitored and recorded within the table game server in an un-editable Event History. The server Event History will also contain any relevant events generated by the server.

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.

4.1.11 Accounting Information

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

4.1.12 Report

Terminals shall transmit all financial information and 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.

4.2 System Requirements

4.2.1 System Redundancy

The server shall 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.

4.2.2 Backup & Recovery

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

1. Information on system configuration;
2. Significant Events;
3. Account information including winnings, bets, cash deposits and cash withdrawal and PIN change;
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.

4.3 System Security

4.3.1 Physical Access

The server or system element(s) must be located in a secure locked area where access is limited to authorized personnel. 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.

4.3.2 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 user name/ID).

4.3.3 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 shall 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.

4.4 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.

4.5 Communication Protocol

1. All protocols must use communication techniques that have proper error detection and/or recovery mechanisms which are designed to prevent unauthorized 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.

4.6 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 the Commission Standards.
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 the Commission Standards.
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.

4.7 SATG Requirements

The following requirements are applicable only to SATGs:

1. 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.

5 PLAYER PROMOTION / BONUSING SYSTEM

5.1 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.

5.2 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).

5.3 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.

5.4 Player Promotion System Requirements

5.4.1 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*[4].
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.

5.4.2 Player accounts maintenance

1. Storage of account data must be secured against invalid access or update other than by approved methods.
2. All adjustment transactions are to be maintained in a system audit log.

[4] 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 must only be kept and stored in an encrypted form in transit and at rest. The encryption must meet cryptographic standards equivalent to the standards set out for encryption in the 'Australian Government Information and Communications Technology Security Manual (ISM) – Controls'.

5.4.3 Database Security

Security of player information, player entitlement and transactions must be guaranteed at all times (e.g. prevention of unauthorized access).

5.4.4 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.

5.4.5 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.

5.4.6 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 (i.e. player's machine credits balance).

3. The player account balance (i.e. player's machine credits balance) must be used solely for game play redemption activities on gaming machine devices.

4. Procedures must be in place to handle "stolen" card/account by invalidating the account and transferring all balances into a new account.

5. 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.

6. Any changes to the player promotion scheme must be logged and auditable.

7. Any manual adjustments to the player's account balance must be logged and auditable.

8. 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).

9. 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 the Commission Standards.

10. The promotion system must be included in the CMS baseline and subjected to CMS software verification and external integrity authentication.

5.5 Player bonusing System Requirements

5.5.1 Database Security

Security of bonusing parameters, player bonus awards and transactions must be guaranteed at all times (e.g. prevention of unauthorized access)

5.5.2 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.

5.5.3 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 the Commission Standards.

6. The bonusing system must be included in the CMS baseline and subjected to CMS software verification and external integrity authentication.

6 NETWORK AND COMMUNICATION REQUIREMENTS

6.1 Cryptographic Data Security

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

6.1.2 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.

6.1.3 Encryption Algorithm Approval

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

1. Encryption algorithms are to be demonstrably secure against cryptanalytic attacks and must confirm 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.

6.1.4 Message Authentication Algorithm Approval

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

6.1.5 Encryption Keys

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

6.2 Communications Requirements

6.2.1 Data Communications Protocol

1. Commission approval must be obtained in advance for any protocol used for 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. Crown System Equipment must be recoverable to the point of failure following an interruption.

6.2.2 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. The Commission will determine exact requirements depending upon the Victorian casino's system design.

6.2.3 Network Baseline

6.2.3.1 Introduction

Network Baseline (Baseline Envelope)

During the approval stage of a system network, and based on the System Document prepared by the Licensee, together with the assistance of the tester, the Licensee and the Commission will determine the core areas of the system network that it will maintain verification control over and this will be defined and approved in the **Network Policy Document**.

Network Policy Document (NPD)

The document is essentially a matrix of Baseline Components and First Tier Non-Baseline Components that describes the network topology of the system, details of the permitted or denied modules, interconnections within the network and the type of connections permitted.

Submissions associated with changes to the NPD must include the current System Document.

6.2.3.2 Physical Requirements

1. Power to devices inside and on the boundary of the baseline envelope must be provided from a filtered, dedicated power circuit. As a minimum standard, this requirement applies to any 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.

6.2.3.3 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.

6.2.3.4 Connection of External Devices to Networks within a Baseline Envelope

1. Unused ports on network devices and network control devices inside and on the boundary of the baseline envelope are to be disabled.
2. Configuration changes to all devices inside and on the boundary of the baseline envelope must be password protected. Password protection policies, procedures and standards must exist and be implemented by Crown, 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 enter.

6.2.3.5 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.

6.2.3.6 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 Crown.
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.

6.2.3.7 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 at the boundary or inside the baseline envelope.

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

6.2.4 Computer Monitoring Systems and Network Management Systems

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

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

3. The configuration of monitoring tools and network management systems must not be changed without formal authorisation consistent with Crown's access and security procedures. Automatic verification of the configuration of these systems must be performed at least daily.

4. 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.

5. 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.

6.2.5 Verification Tools

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

7 SUBMISSION REQUIREMENTS

7.1 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. Crown'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.

7.2 Player information

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

7.3 Communications

7.3.1 Authentication and Encryption

1. Crown must provide details of the message authentication algorithm used.
2. Crown 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.

7.3.2 Internal Network Architecture

1. Crown 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. Crown must provide details of any remote connections used (if any) to support CMS operations.

3. Crown must provide details of authentication and encryption associated with remote connections.

4. Crown 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, Crown 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 access to other information on Crown;
   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. Crown must provide details and configurations of the devices that will be used to control access from other networks (including non-production networks used by the operator) to the internal production network.

7. Crown must provide details of controls and audit trails associated with access and modifications to network components.

8. Crown 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.

7.3.3 Third party connections

1. Crown 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, Crown 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 access to other Crown 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.

7.4 CMS Infrastructure

1. Crown must provide an overview of the CMS design.
2. Crown must provide a functional specification of the CMS.
3. Crown must provide detailed CMS design documents.
4. Crown 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. Crown must provide descriptions of where and how information is stored throughout the system.
7. Crown must provide detailed descriptions of its password protection systems and associated algorithms utilized by the system.
8. Crown must provide a description of the method of transaction logging used.
9. Crown must provide details of situations during which encryption of data files will be employed.
10. Crown must provide a description on how self-monitoring is to be implemented.

7.5 CMS software

7.5.1 Open Source Code

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

(a) Source code files;

(b) Make or batch files;

(c) Map files;

(d) Master images; and

(e) Any other files used in conjunction with the master images.

7.5.2 Closed Source Code

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

(a) Master images from the closed-source development environment, and

(b) 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.

7.5.3 Compilation Environment

1. Crown and/or suppliers of the CMS must provide the Commission or an authorized tester 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. Crown must provide a description of the method to be used to verify the integrity of the software operating on the production CMS.
9. Crown and/or suppliers of the CMS must provide commission or an authorized tester copies of operator's manuals, operator's procedures manuals and system administrator manuals or equivalent.

7.6 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. A l 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.

8 GLOSSERY OF TERMS

Term or Abbreviation	Description
CMS	The Casino Monitoring System made up of the Host Monitoring System, Jackpot Systems, Electronic Table Games and Bonuses & Promotions systems required for the operation in Crown Casino in Melbourne.
Commission	The Victorian Commission for Gambling and Liquor Regulation established under the Act or any successor body.
Commission Standards	The relevant Commission gaming standards consisting of: 1. Australia/New Zealand Gaming Machine National Standards, 2. Victorian Appendix to the Australia/New Zealand Gaming Machine National Standards; and 3. Victorian Casino Monitoring system requirements (this document)
Critical Memory	Memory locations storing information that is considered vital for the continued proper operation of the CMS.
EGM	Electronic Gaming Machine – has the same meaning as Gaming Machine
Protocol	The means for communication between the EGM and CMS
Firewall	Part of a computer system or network that is designed to block unauthorized access while permitting authorized communications
PIN	Personal Identification Number
Pre-Commitment	A mechanism to allow players to stay in control of their gambling and make informed decisions about their play
SIA	Security Integrity and Authentication process. This process is to validate and verify the System Baseline executable files (and selected command utilities) in order to confirm that the configuration of the system is operating in an approved state.
VCGLR	Victorian Commission for Gambling and Liquor Regulation