vgccc
Victorian Gambling
and Casino Control
Commission

Victorian Lottery System Requirements

OFFICIAL: Sensitive

July 2018

Version: 2.0

VICTORIA
State
Government

vgccc.vic.gov.au

Table of Contents

1   Glossary

This chapter sets out the glossary of standard terms and abbreviations used by the Victorian Commission for Gambling and Liquor Regulation (the Commission) and relevant to the Victorian Lottery System Requirements document.

Term or Abbreviation	Description	
Act	The *Gambling Regulation Act 2003*.	
Agent	A person engaged under an agreement, or appointed as an Agent of the Licensee under an agreement, to assist in the conduct of an Authorised Lottery.	
Ancillary Agreement(s)	Means an agreement entered into by the Minister and the Licensee in accordance with section 5.3.7A of the Act.	
Authorised Lottery	Means each Public Lottery that the Minister has authorised the Licensee to conduct.	
Baseline	A snapshot of an evolving system. The baseline also defines an envelope around a system (defined by the Licensee and approved by the Commission) which the Commission maintains verification control over the Victorian jurisdictional components. For example, application files within a baseline would need approval prior to being modified, and there must be a method in place to verify Baseline files have not changed since the last approval.	
Commission	The Victorian Commission for Gambling and Liquor Regulation established under the VGCCC Act.	
Configuration Management	The process of creating and maintaining a record of all the components of the infrastructure, including Hardware, software and related documentation, and managing changes to the attributes of the components.	
Critical Data	Information including, but not limited to: security events ticket serial numbers RNG seeds signature seeds (algorithm coefficients) signature results encryption keys	PINs passwords software uploads and downloads of any security related software transfer of money between computer equipment, any changeable configuration information unclaimed tickets.

Cryptographic Data Security	Refers to the protection of critical communication data from eavesdropping and/or illicit alteration.
Data	Means all data and expressions of data contained in, or processed or generated by, the Lottery System including without limitation: all data and expressions of data comprising reports generated by the Lottery System all data and expression of data about or relating to or generated by Agents and contractors stored within the Lottery System.
Distributor	Means any person appointed or engaged by the Licensee to accept from a Player an entry or payment for an entry to an Authorised Lottery.
Firewall	Part of a computer system or network that is designed to block unauthorised access while permitting authorised communications.
Hardware	All physical components (electrical and mechanical) making up the Lottery System equipment.
Help Desk	A service by the Licensee that provides information and assistance to Agents, Distributors, the general public, Players and support teams.
I/O Channel	The physical interface that controls the transfer of data between the computer and peripheral devices.
ICT	Information Communications Technology – a generic name used to describe all technologies used by computers to communicate.
Inspector(s)	A person who is appointed under Part 4 section 40 of the VGCCC Act to represent the Commission in undertaking inspections of the Lottery System.
Instant Lottery	A Public Lottery where the result, prize and winning Player(s) are not determined by an independent or separate draw or event held or occurring sometime after the time of purchase of a ticket or entry in the lottery.
LAN	Local area network is a computer network that interconnects computers and devices within a limited area.
Licence	Means the Licence granted and issued under the Act by the Minister to authorise the conduct of authorised Public Lottery activities.
Licensee	The holder of the Licence granted and issued under the Act by the Minister to authorise the conduct of authorised Public Lottery activities.
Lottery Rules	Has the meaning given in section 5.1.2 of the Act.
Lottery System	The technical systems necessary for the Conduct of Authorised Public Lotteries in accordance with the requirements of the Licence and the Ancillary

	Agreement and approved by the Commission in accordance with section 5.2.1A(1) of the Act.
Mechanical RNG	Means a device used to generate random results, excluding computational devices. Examples of mechanical random number generators are: roulette wheels, dice and/or ball draw machines.
Memory	An area of a computing device used to store data and/or instructions.
Minister	Minister responsible for administering Chapter 5 of the Act.
Network Policy Document	A document describing the end-to-end network topology of the Lottery System which is the responsibility of the Licensee to prepare as part of its submission to the Commission when obtaining approval for the Lottery System.
OLGR	Office of Liquor, Gaming and Racing within the Department of Justice & Regulation.
PCI	Payment Card Industry
PCI compliant	Indicates compliance with the Payment Card Industry Data Security Standards, as set by the PCI Security Standard Council.
PIN	Personal identification number.
Player	Means a person who enters an Authorised Lottery.
Public Lottery	Has the meaning given in section 5.1.2 of the Act.
Random Number Generator (RNG)	Means a computational or physical device designed to generate a sequence of numbers or symbols that cannot be reasonably predicted better than by a random chance.
Roll of Manufacturers, Suppliers and Testers (the Roll)	Means the Roll of Manufacturers, Suppliers and Testers established under section 3.4.60 of the Act.
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.
System Baseline Document	Document detailing the system software and Hardware components and network and communication that enable the system to operate in a secure environment and meet the legislative requirements.
Tester	A tester listed on the Roll as described in Chapter 3, Part 4, Division 7 of the Act, that operates an Accredited Testing Facility.

VGCCC	The Victorian Commission for Gambling and Liquor Regulation.
VGCCC Act	The *Victorian Commission for Gambling and Liquor Regulation Act 2011*.
Victorian Government	The State Government of Victoria.
VLSR	Victorian Lottery System Requirements (this document).
WAN	Wide area network: a computer network that covers a broad physical area.

2   Foreword

This chapter introduces the background to the Victorian Lottery System Requirements document.

2.1   Lottery framework

Public Lotteries in the State of Victoria operate under a Licence issued by the Minister pursuant to Chapter 5 of the Act.

The Licensee is required to conduct Authorised Lotteries, which may include Instant Lotteries, during the term of the Licence in accordance with the:

- *Gambling Regulation Act 2003* (the Act)
- conditions of the Public Lottery Licence and terms of the Ancillary Agreement or any other related agreement entered into by the Licensee and the Minister
- Lottery Rules applicable to each Authorised Lottery.

The Commission regulates the Authorised Lotteries conducted by the Licensee, which includes the approval of products, system and Lottery Rules, monitoring of the data and system integrity of the Authorised Lotteries, via systems, and financial and compliance assurance processes.

3 Introduction

This chapter introduces the context and the purpose of the Victorian Lottery System Requirements document.

3.1 General information

This document:

- must be read in conjunction with the Act, the Licence and the Ancillary Agreement.
- contains the system-related requirements for the Lottery System.
- is a standard pursuant to section 10.1.5A of the Act, and is the "Commission's Technical Standards" as referenced in the Public Lottery Licence Ancillary Agreement.
- is to be used by the Licensee and Tester(s) to evaluate the Lottery System for compliance with these requirements, and any subsequent changes to a previously approved system.
- will also be used by the Commission to evaluate compliance by a Licensee with the Licence and any Ancillary Agreement(s), and to evaluate any subsequent changes to a previously approved Lottery System, in accordance with the Act.

It may be necessary to amend conditions of this document from time to time, which will be performed by the Commission in consultation with the Licensee.

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

3.1.1 The Act

This document does not take precedence over the Act. To the extent of any inconsistency between this document and the Act, the Act prevails.

3.1.2 Objectives

The Commission sets high integrity standards for Lottery System(s) in relation to Public Lotteries offered in Victoria for the purpose of ensuring that:

- the system operates in accordance with the Licence and any Ancillary Agreement(s)
- the system operates in accordance with the approved Lottery Rules
- the system is fair to Players
- all parties receive the correct entitlement from lottery subscriptions and revenue
- the system operates in a manner that is auditable, reliable and secure.

Matters arising from the testing of the Lottery System that have not been addressed in this document will be resolved at the sole discretion of the Commission as part of the approval process. In considering any new technology or omissions, the Commission may take into account advice on such matters from either a Licensee, a Tester, or other third parties deemed necessary.

3.1.3   Document scope

The requirements in this document apply to the Lottery System, including all components, to be operated by the Licensee according to the Licence and any Ancillary Agreement(s) at central locations and Distributor's businesses in Victoria.

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

To this end, any submission which includes new technology and/or is not adequately addressed by this document must include an analysis and description of the testing approach (and rationale) and techniques that will be used by the Tester.

3.1.4   General principles

The Lottery System must fully implement the requirements and services as specified in the Licence and any Ancillary Agreement(s).

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

3.2   Operational requirements

3.2.1   Provision of information

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

When evaluating the Lottery System for approval, the Licensee must provide sufficient information and documentation to enable a full determination of the Lottery System's level of compliance with the VLSR.

3.2.2   System performance standards

The Lottery System must be capable of meeting the performance standards set out in the Licence and any Ancillary Agreement(s) and the requirements set out in this document and any other relevant standards, specifications or conditions determined by the Commission, with an expected System availability of at least 99.95% excluding the exceptions permitted in Schedule 3 (Section 1 (b)) of the Ancillary Agreement.

Communication systems forming part of or used in association or connection with the Lottery System must be capable of meeting the performance standards set out in the Licence and any Ancillary Agreement(s).

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

The Lottery System must be capable, at all times, of determining whether all agreed upon Lottery System components and peripheral equipment connected to it are functioning.

3.2.3   Responsibilities

The Licensee must adhere to the responsibilities detailed in the Act, the Licence and any Ancillary Agreement(s).

3.2.4   Service management framework

In order to ensure that the Lottery System (services and associated equipment) operate as approved by the Commission, the Licensee must establish and maintain policies, standards and procedures that the Licensee will use to develop, implement and operate the Lottery System. These policies, standards and procedures will be part of a structured service management framework operating under industry best practices, such as ISO 9000 or an equivalent standard.

ICT service management framework

ICT service delivery forms a major component of the overall service delivery. ICT services should include (but not are limited to):

- a service support function which incorporates:
  - incident management
  - problem management
  - Configuration Management
  - change management
  - release management
- a service delivery function which incorporates:
  - availability management
  - capacity management
  - service level management
  - service continuity management
- security management
  - the Licensee must establish and maintain Information Security Management Systems that meet ISO/IEC 27001:2013 or an equivalent standard.
- ICT infrastructure management (Hardware and software)
  - design, deployment and operational management of ICT equipment and software in the provision of the Lottery System as approved by the Commission
- application management
  - the ongoing management of all Lottery System applications which will include but not limited to: designing, testing, operating, improving and support.

A service desk function, which incorporates a structured Help Desk that manages all service and incident resolution requests must be able to handle any questions, problems, disputes and maintenance calls. This service is to be provided to all entities which interact with the Lottery System, including Players, participating Agents, Distributors, the public and the Commission.

4 Lottery System control

This chapter sets out the Victorian Lottery System requirements that must be met for the Licensee's operation in Victoria.

4.1 Lottery System environment

The Commission requires that the Licensee implement a computerised system capable of meeting the following broad functions including, but not limited to, the ability to:

- support the requirements/conditions of the Lottery Rules, Legislation, the Licence and any Ancillary Agreement(s)
- support the predicted system load requirements
- provide adequate system audit and security requirements
- provide adequate financial verification and audit capabilities
- provide reports as required by the Commission.

The Lottery System must be a computer-based system with sufficient capacity (processing, Memory, communications interfaces and storage) to efficiently perform all tasks associated with providing a Public Lottery.

The Lottery System must be capable of operating 24 hours a day, seven days a week throughout the term of the Licence, and as required by the Licence, with an expected System availability of at least 99.95% excluding the exceptions permitted in Schedule 3 (Section 1 (b)) of the Ancillary Agreement.

The Licensee must notify the Commission of any planned system downtime, whether scheduled or non-scheduled. The Commission must be notified in advance of all planned system downtime in a manner and in time frames as determined by the Commission. The Commission retains discretion to develop notification procedures. Such notification procedures may involve:

- explicit prior approval by the Commission
- notification with possible disallowance, or
- notification with an understanding that the Licensee may proceed without response from the Commission.

If the Commission disallows the downtime or does not approve the downtime, the Licensee must not proceed with the downtime. Logs and records must be retained for all downtime.

The Lottery System is deemed to extend to the point at which the Authorised Lottery is offered to the Players.

The system must not result, either directly or indirectly, in an exclusive arrangement for the operation of Agent management systems beyond the minimum system requirements necessary to offer the Authorised Lotteries of the Licensee.

4.1.1 System Useability

- The Lottery System shall be designed in consideration of the following usability principles:
- Visibility of system status, keeping users informed through appropriate feedback within reasonable time
- Words, phrases and concepts familiar to the user, rather than system-oriented terms, in a natural and logical order

- Facility to correct a mistake (undo or redo the action) without having to go through an extended dialogue
- Platform conventions that ensure words, situations, or actions mean the same thing
- Design that prevents error-prone conditions or checks for them and presents users with a confirmation option before committing an action
- Minimise the user's memory load by making objects, actions, instructions and options visible or easy to retrieve whenever appropriate
- Flexibility and efficiency of use through design that caters to both inexperienced and experienced users and allows users to tailor frequent actions
- Aesthetic and minimalist design that excludes information that is irrelevant or rarely needed
- Help for users to recognise, to diagnose, and to recover from errors including error messages that are expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution
- Help and documentation that is easy to search, is focused on the user's task, and lists concrete steps to be carried out.

The Lottery System shall be designed in consideration of the *Victorian Government Website Management Framework – Accessibility standard.*

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

- changes in requirements and standards (as determined from time to time by the Victorian Government and the Commission)
- advances in technology
- configurable items.

4.2   Lottery System Hosting

4.2.1   Physical security

The host Lottery System computer room(s), including RNG's, must be a secure area that can only be accessed by authorised personnel. The Commission requires the use of an electronic locking system that provides monitoring/logging information on access events by personnel.

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

There must be a detection system that securely records audit events associated with any physical access (or attempted access) to the host Lottery System(s) and components. An alert must be generated and actioned upon for unauthorised activity.

The Licensee must, prior to the commencement date of the Licence and at regular intervals, ensure that an accredited external and independent security testing company undertakes testing of the physical security of the computer room(s) and related Lottery System equipment and provide a written report of its findings. This report must be provided to the Commission within two weeks of its receipt and must include details of action(s) taken, and planned actions, by the Licensee with respect to all issues identified in the report.

Lottery System Hosting datacentre support equipment

All host Lottery System equipment within or contributing to the computer room(s) environment must meet best practice industry standards in data centre practices. Some of the hosting requirements include, but are not limited to:

- redundant power supply
- uninterruptible power supply
- stand-by generator
- emergency lighting
- fire suppression
- environmental control system.
- secure server cabinets.

The RNG device's physical security has additional requirements as specified in other sections of this document.

4.3 Service desk

The Licensee must provide a suitable service desk function to assist participating Agents, Distributors, Players, the public, the Commission and any user with questions, problems, disputes and maintenance calls.

All requests to the service desk must be logged electronically and the log made available to the Commission upon request. The information recorded in the system log must include, but is not limited to:

- the time and date the call was made to the Help Desk
- the Agent and/or person making the call
- the issue prompting the call
- details of the outcome of the call.

4.4 Lottery System

The Lottery System includes the technical systems necessary for the Conduct of Authorised Public Lotteries in accordance with the requirements of the Licence and the Ancillary Agreement and approved by the Commission in accordance with section 5.2.1A(1) of the Act.

The assessment of the system will evaluate it for functionality, reliability, recovery, auditability, redundancy, and security.

4.4.1 System Validation

Handshake and signature checking

The Lottery System is required to ensure the presence and connectivity of all critical components.

Where Distributor equipment includes Lottery System approved software, a signature check process is required on power up of the device.

Where a handshake or signature-checking process fails to meet operational criteria a record of the event is to be logged for monitoring and analysis purposes, and the equipment should not activate or "go live".

4.4.2 Configuration Management

The Licensee must have a structured Configuration Management system to control all configuration items within the Lottery System.

System Baseline Document

The Licensee must prepare and maintain a System Baseline Document, which contains all attributes and components of the approved system. The document is subject to initial approval by the Commission, and must subsequently be kept current and made available to the Commission upon request.

The System Baseline Document must include:

- system Hardware components
- system application/software components
- network and communication infrastructure components.

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

- communicate with the Baseline envelope components
- share Hardware or database instance with Baseline components.

The Licensee must submit to the Commission as part of system approval, the following:

- documentation on all system components
- documentation on all system component related configuration items
- recommendation provided by a Tester.

The system Baseline and the System Baseline Document must include all the core components of the Lottery System, including, where applicable:

- the software used to validate and verify that the system is operating in an approved configuration
- application files including database stored macros and/or scripts and procedures
- Hardware platforms
- operating systems
- interface devices/modules and related software that interact with databases used by the system application
- interface devices and related software that interacts with any application, external system, Agent/Distributor or third party services
- systems communication devices that interface with any application, external system, Agent/Distributor or third party services or equipment
- identification of any operations or procedures relevant to securing and controlling of the system
- identification of any other special operational or procedural issue that is relevant to the Commission.

The System Baseline Document must specify the location of application files and configuration files.

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

All system network connection and configuration interfaces must be identified and represented in the Network Policy Document.

4.4.3 Change Management

Standard change requirements

The Licensee must obtain the approval of the Commission for changes to any components identified within the Baseline.

Each application for a change to the Baseline must include a revised System Baseline Document for verification and endorsement by the Commission.

Each application for a change to the Baseline must be accompanied by a Tester's recommendation, or as per arrangements agreed with the Commission.

Emergency changes

A licensee can implement an emergency change to the approved Lottery System in line with set criteria determined in this document. An emergency change, which meets the criteria set out below and follows the required notification processes, will then require a formal approval in line with the process for ordinary system changes. Failure to notify the VGCCC or process a change in line with the set criteria below will deem the licensee as operating an unapproved Lottery System.

Definition of an Emergency Change

A change is classified as an Emergency Change when the risk or potential impact of not immediately implementing the change is considered critical, in order to:

- maintain player fairness,
- ensure all parties receive their correct return, through accuracy of gambling returns and reported data
- ensure security, integrity, or auditability, and failure to repair may impact player confidence, OR
- ensure adherence to legislative requirements.

In the event that the licensee is uncertain as to the legitimacy of what it considers to be an emergency change in line with the criteria above, a formal request for confirmation of this must be sought via email to the level 2 stakeholders noted below.

The VGCCC will endeavour to respond in a timely manner to acknowledge the legitimacy of the emergency change if required. If such acknowledgement is required, please allow 24 hours for the VGCCC to consider the change. If the VGCCC is unable to provide a decision within 24 hours the licensee may progress the emergency change.

Stakeholder definition

All "Document Stakeholders" must be identified as Role/Position Title, Team and Department name within each document.

Level 1

All Level One Stakeholders approve all major changes to their document/s, including:

- Senior Manager – Team/Department
- Manager – Role/Title

Level 2

All Level Two Stakeholders are notified of all baseline changes, including:

- Internal stakeholders and change management facilitators
- VGCCC contacts as specified in writing by the Commission

Components of the Emergency Change Process

The Emergency Change process initiated by the major licensee must consist of, but is not limited to:

- Change number, or reference

- Before and after software version numbers
- Detailed description of change, include clear justification of how the licensee has determined that the change meets the above criteria
- Implementation date and time
- Name and position of staff authorizing the change
- Signatory of staff authorizing the change
- Date and time the change was authorized
- Name of VGCCC officer contacted
- Date, time and mode of contact
- CRC of system file(s) before change
- CRC of system files after change
- Baseline Global CRC before change(s) and
- Baseline Global CRC after changes.

Prerequisites of the Emergency Change Process

Emergency Changes to the regulated System Baseline require the following steps to be initiated internally by the relevant licensee:

- Approval must be granted by the relevant internal officer and evidenced on the change notification advice
- The VGCCC must be notified of the change prior to implementation
- The VGCCC must be notified upon completion of the Emergency change and
- Subsequent formal approval must be sought from the VGCCC via the standard approval process.

Note: It is a VGCCC requirement that before any software baseline change is initiated, a CRC (or agreed software verification tool) verification is undertaken to confirm that the software to be amended accords with the software approved for use by the VGCCC. Following all software baseline changes a CRC verification is to be performed to ensure that a record is created of the changed CRC baseline list, and that only those files required to address to the Emergency Change have been modified.

Notification process for an Emergency Change

In providing notification to the VGCCC, before the initiation of any emergency change, the responsible internal officer within the Licensee must:

1) Contact via phone (or email if phone contact is unavailable) key Level Two VGCCC stakeholders as noted above. A clear verbal notification of ALL components of the emergency change must be evidenced in the conversation; and

2) Email a copy of a formal notification form, addressing ALL points identified in 2.1 above, as determined by the licensee.

Within 24 hours of implementing the change, the Licensee must formally provide the VGCCC with confirmation of the change in line with the initial notification provided. Any deviation from the initial notification in relation to the emergency change must be evidenced in the communication. Appendix A provides details of the documentation that must be submitted to the Commission after emergency changes have been implemented.

Approval of the system incorporating the Emergency Change

A copy of the notification form provided to the VGCCC must also be provided to the Accredited Testing Facility to assist in certification of the emergency change.

The subsequent request for approval of an Emergency Change to the baseline must be submitted together with the next submission for a change to the System baseline, if there is a system version upgrade scheduled within one month. If not, the change is to be formalised within 30 days of the emergency change. In the case of a scheduled change, the Tester's report(s) should attest for the scheduled change and the emergency change holistically. It is not acceptable to submit separate test reports that do not at least cross reference one another.

It is expected that there will be no further emergency changes before formalisation of the approval.

No new functionality should be introduced with the subsequent emergency change approval submission, unless it is part of a scheduled system release.

The Tester recommendation must include the following information:

- The new CRC's of any modified baseline application files (or scripts)
- Information on the disabling of any system functions such as logs, encryption, and when the action took place (and a note to say when it will be re-enabled, if applicable).
- Any significant modification to any system.
- A statement that the changes recommended formalises the Emergency Change (Change Number & date of Emergency Change).

4.4.4   Lottery system service delivery procedures

The Licensee must establish and maintain policies, procedures and standards in accordance with the operational requirements referenced in this document.

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

If unapproved, non-baselined, application files reside on storage devices on in the Memory of identified Lottery System Components, these should be identified in the Baseline document, and identified as non-baseline.

4.5   Central logging of information

All Lottery System associated audit logs, financial data and significant events data must be retained and be able to be accessed or retrieved (either online or from back-up) for seven years from the day the log or data was created.

All Lottery System associated audit logs, financial data, significant events data and drawn numbers data must be available on request to assist the Commission with audits and investigations.

4.6   Significant events

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

Significant events are those events deemed significant by the Commission and may include, but not limited to:

- system downtime
- signature failure of any Baseline component of the Lottery System
- system security access breach
- RNG failure
- incorrect dividend calculation

- communication failure with the RNG.

4.6.1 Detection of significant events

The Licensee must determine an appropriate method of implementation for the detection and recording of significant events.

4.6.2 Recording of significant events

Records of significant events are to be stored securely in the Lottery System.

Records of significant events must be stored electronically in a manner approved by the Commission.

A date and time stamp (when the event occurred) must mark each record in the file and it must be able to be retrieved.

Significant events must be logged/stored in a timely manner.

4.7 Lottery system security

Security management

The Licensee must establish and maintain policies, procedures, standards and mechanisms for adequate security over the approved system to ensure continued system integrity, availability, and auditability.

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

Application Access

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

- initial password change on its first use must be enforced
- an appropriate password policy must be enforced that is agreed between the Licensee and the Commission
- procedures for adequate protection of passwords.

Security Reporting

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

- access a system account
- access a user account
- access system resources
- view or change system security definitions or rules
- add, modify or delete critical system data
- access Mechanical RNG devices
- change security configurations
- access secure locations utilised in the conduct of lotteries, both physically and/or logically.

In addition to the above, exception reporting must include, but is not limited to, a method of detecting:

- irregular patterns of use for system or user accounts
- significant authorised changes to security configuration.

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

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

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

It must be possible (electronically) to list all registered users on the system including their access level and a record activity history by the registered user which must be kept current.

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

- system parameter changes
- installation of new versions of software
- other functions as determined by the Commission.

The Licensee must develop and maintain policies and operating procedures to prevent unauthorised access or changes to the Lottery System and related equipment.

The Licensee must maintain its system security in line with ISO/IEC 27001:2013.

The Licensee must ensure that an accredited external and independent information technology network and security testing company undertakes system and network penetration testing at appropriate intervals or at a minimum every two (2) years after the commencement of the Licence.

The penetration test must include, at a minimum scope, internal and external penetration tests. (Refer to the *Victorian Government Enterprise Solutions SEC GUIDE 03 Information security penetration testing guideline*).

The system and network penetration testing report must be provided to the Commission within two (2) weeks of its receipt and must include details of action(s) taken, and planned actions, by the Licensee with respect to all issues identified in the report.

4.7.1   Auditability of the Lottery System

The Licensee will be subject to regular compliance and system audits by the Commission or an Inspector.

The system audit will assess the security and controls over the system to ensure that the system is operating as approved by the Commission and integrity of Lottery System and data is maintained at all times.

The scope of the audits includes but is not limited to:

a)   logical access security and control such as user access creation, user and access privileges reviews, generic accounts security and controls, remote access control and management

b)   physical and environment security such as data centre access controls, RNG security and control

c) system integrity such as approved components Baseline verification for compliance, source code integrity, regular monitoring of critical activities of the system and its components with preventive, detective, and corrective controls in place

d) data and information security and integrity such as database security and control, financial data integrity, customer data and information integrity

e) game resulting and outcome integrity such as security and controls of draw process and procedures, RNG, unclaimed lottery tickets

f) networks and communications security such as regular Network Policy Document reviews, prevention, detection and correction measures for relevant security breaches

g) software, Hardware and network change management and deployment such as emergency change and Configuration Management

h) problem and incident management including significant events management

i) system availability such as backup security and controls by regular testing of retrieval and restore from backup devices, storage management records

j) business continuity management such as disaster recovery and business continuity planning, testing and documentation

k) asset management such inventory management of approved components

l) system interfaces and peripheral equipment integrity

m) accountability maintained by appropriate segregation of duties

n) adequate audit trail maintained for accountability, reconstruction, intrusion detection, problem detection

o) system and audit log monitoring including appropriate procedures for follow-up and corrective action

p) adequate audit trail and logs kept to help in auditing through the computer as for customer complaints and investigation

q) availability of adequate policies, procedures and standards, which are regularly followed, maintained and kept up to date.

4.8 Lottery system back-up and recovery

4.8.1 Host Lottery System recovery

The Licensee must have policies, procedures and standards in place in accordance with Commission guidelines for hosting Lottery System data and software back-up and recovery and any relevant components.

4.8.2 Transaction logging

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

The host Lottery System must record in a log file or databases (including time stamp and date stamp) all critical or relevant lottery transactions received from Lottery System equipment and other elements of the Lottery System.

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

The method of transaction logging will be assessed by the Tester and considered by the Commission as part of the system approval.

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

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

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.

4.8.3   Format of records

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:

- the date that the transaction/event occurred
- the time that the transaction/event occurred
- the identifier for the part of the Lottery System for which the transaction/event occurred
- any relevant data that is associated with the event
- a unique event identifier that defines the transaction/event.

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

4.8.4   Disaster recovery (DR) and business continuity

The DR site must meet the standards required for the primary site as set out in this document and approved by the Commission.

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

The Licensee must ensure that a DR site(s) is retained, tested and operational at all times to ensure business continuity.

The Licensee must establish and maintain systems consistent with the primary site, including policies, procedures and standards for business continuity and disaster recovery.

The Licensee must establish and maintain a DR test plan, including a schedule for testing – that must be approved by the Commission – and conduct DR testing in accordance with the approved plan.

In the event of a disaster, there must be a method of ensuring that all data, transactions and information related to the Lottery System are preserved up to the point of the disaster.

Copies of all 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.

There must be sufficient back-ups of the variable database files on the host Lottery System storage devices to ensure the restoration of services without data loss.

4.8.5 System data recovery

In the event of a failure whereby the host Lottery System cannot be restarted in any other way, it must be possible to reload the system from the last backup point and fully recover all data including at least all of the following critical or relevant transactions:

- significant events required to be stored in the Lottery System
- manual database updates
- audit logs
- current system encryption keys
- records of lottery draws
- lottery entries, including financial data.

The solution must support standard and emergency data recovery requests.

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

4.8.6 Central site failure modes and recovery

Following any failure, it must be possible to restore the state of the host Lottery System and its database(s) without losing data.

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

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

- processor
- computer power supply
- computer Memory
- computer disk(s)
- computer I/O Channels
- power supply of the central site
- operator (invalid data entry, etc.).

4.9 Data security

4.9.1 Encryption of stored data

The Licensee must encrypt stored system related data and the encryption used must meet cryptographic standards equivalent to the standards set out for encryption in the '*Australian Government Information and Communications Technology Security Manual (ISM) – Controls'*.

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

- PINs
- passwords.

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

- encryption / decryption keys

- unclaimed tickets.

4.9.2   PIN and password management

If a Lottery System operator's PIN or password is used in support of the system, the PIN or password creation algorithm, its implementation and operational procedures (pertaining to PIN and password changes, database storage, security and distribution) will be assessed as part of the Commission approval of the Lottery System.

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

4.10   Lottery System integrity

4.10.1   Configuration Management

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

The Commission's assessment of the Lottery System will include, but not limited to, an evaluation of the Hardware configuration for operational integrity as well as reliability, recoverability, audit ability, redundancy, and security.

4.10.2   Security of event and transaction logs

It is mandatory that the event log and software is structured so that it is not possible for there to be unauthorised modifications. This will involve both password security control and ensuring that the only valid method of writing to the events log is output sequential (that is no random update methods are to be permitted).

4.10.3   Multiple log files

There must be at least two physical copies for each file and/or database that contains the vital information (as defined in this requirements document) using secure storage methodology.

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

4.10.4   Data and event collection

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

4.11   Documentation and reporting

The system must be able to provide data and system reports in a form determined and requested by the Commission.

4.11.1   Required reports

The Commission must be satisfied that:

- the information printed or displayed is accurate
- the user interface and operation of the system is presented, both by the system and in documentation (operators' manuals, etc.), in a manner which is conducive to efficient operation of the systems.

Reports and data to be supplied to and agreed by the Commission, will include printed and/or electronic formats.

The system must provide, but not limited to, the following information:

- total sales by draw
- subtotal sales (break-up by product)
- subtotal by state and overseas jurisdictions
- Player loss by draw, by state and overseas jurisdiction
- declared dividends by draw
- all jackpot reports by draw
- all revenue and tax reports by draw
- financial alteration reports showing any amounts changed (and who/when performed the changes)
- real time game closure/snap reports for audit to perform game closure verification
- system dividend share reports.

4.11.2 Lottery System interfaces to sub-systems

The Commission must approve the integration of all sub-systems or utilities with the Lottery System in general, including:

- performance monitoring systems
- security systems
- network communication and monitoring
- application management systems
- environmental monitoring systems
- any other application that is assisting in the efficient operation of the Lottery System.

The integration of the Lottery System with sub-systems or utilities must be described in the Configuration Management plan.

4.11.3 Lottery system terminal functions

Commission approval must be obtained for all lottery terminal functions pertinent to Public Lottery games.

All terminal functions not pertinent to public lotteries must not interfere with or affect the outcome of Public Lottery games or any terminal functions that are pertinent to the Public Lottery Games.

Commission approval must be obtained for the method and security of communications to and from a lottery terminal.

4.11.4 Access by the Commission to the Lottery reporting system

The Licensee, at the direction of the Commission or an Inspector, must provide access to the Licensee's computer system.

Access provisions to the Lottery System software must include tools, mechanisms and resources to:

- examine, download or print significant events
- request, generate, review, save and print reports.

4.11.5 Facilities for inspection

Facilities for Inspectors are to include, but not limited to, the ability to:

- independently determine and test operational Hardware and software versions
- review Baseline verifications of executable software upon request
- verify that Lottery System equipment is on-line
- review significant events and reports
- access and review audit logs
- conduct a SIA
- secure Licensee technical assistance to perform all the above
- secure Licensee technical assistance to assist Inspectors in the conduct of technical compliance
- provide other facilities to assist the conduct of Inspectors' tasks as necessary for a particular Lottery System.

4.11.6 Recording of lottery results

When numbers are drawn as a 'result' of the game, these numbers must be recorded to a permanent storage device in a form that can be authenticated to detect any subsequent modification, before communication of the numbers drawn to the central computer is commenced.

Should there be some kind of failure before the central computer has recorded all of the required numbers, the recorded output may be used to manually complete that draw.

The recorded output must include, but not limited to, the following information:

- date
- time
- lottery product code and name
- corresponding lottery product game number
- numbers drawn
- checksum result
- other security information if available.

The recorded output must be held and be able to be accessed or retrieved for seven years.

5   Instant Lotteries

This chapter sets out the equipment requirements in relation to the provision of Instant Lottery products.

The Lottery System must provide for the receipt, distribution, processing, accounting, sale, validation and reconciliation upon closure of all Instant Lottery products.

In relation to the provision of Instant Lottery products, the Lottery System must maintain data in relation to:

- the configuration of the approved Instant Lottery products, including, but not limited to, the prize table, value of the ticket, number of tickets
- sales and prizes won/paid
- active and previously closed products
- Distributor level transactions and statistical data.

The Licensee must ensure that due diligence is conducted into the adequacy of the instant ticket supplier, and ensure strict controls are in place regarding, amongst other things, security, quality control, testing, printing, shipment and storage are assessed. Evidence of an independent test performed in relation to, but not limited to, the adequacy of the instant ticket production, storage and security must be provided to the Commission.

The Lottery System must not retain information in a way that can disclose or identify the portion of unsold winning tickets in relation to Instant Lotteries.

The Licensee must ensure that Distributors are provided with instructions on use of the Lottery System to provide for the sale of Instant Lotteries.

In most instances, all Public Lottery requirements noted in this document apply to the sale of Instant Lotteries.

The Lottery System must have an active control system to account for, and track, instant tickets. This provision also extends to tickets for withdrawn / ceased Instant Lotteries.

6   Distributors requirements

This chapter sets out the equipment requirements for operations carried out within Lottery Distribution points in Victoria.

6.1   Responsibilities

6.1.1   Distributor's Hardware and infrastructure

It is the Licensee's responsibility to install and maintain all Distributor's Lottery System equipment that will include, but not limited to:

- a secure local area network for connecting the Lottery System to the lottery equipment within an agency
- a secure WAN for connecting the Lottery System equipment at the Distribution point to the host Lottery System.

Distributor's equipment must be maintained in accordance with Lottery System approval provided by the Commission.

6.1.2   Distributor operations

It is the Licensee's responsibility to:

- manage the interfaces to the Lottery System equipment at the Distributor
- supply the Distributors with relevant manuals, instructions and training for using Licensee provided equipment within the agency
- supply information necessary to support the sale of the Authorised Lottery, including, but not limited to the relevant game rules and responsible gambling codes.
- provide access to an appropriate service desk facility.

7 Online participation requirements

This section refers to requirements relating to Players placing entries via terminals connected to non-Distributor communication channels – such as the web pages through the internet, website, mobile applications or digital television – for distribution in Victoria.

7.1.1 Security and controls

The Lottery System must prevent online Players from being directed to non-Distributor communication channels of a related entity of the Licensee in another State, Territory or overseas or to another member of a bloc agreement for the purpose of purchasing Public Lottery products.

The Lottery System must not allow for the sale of Public Lottery products not approved in Victoria to Victorian residents.

The Lottery System must be able to distinguish the origin of online sales to allow for accurate distribution of revenue for tax purposes.

Online sales of Public Lottery entries via non-Distributor communication channels must only be sold via the Licensee's website.

Before Public Lottery entry transactions can take place, the Player must login to an existing Player account with account identifier and appropriate security control, - that is via account validation including password or PIN.

It must be possible for the Player to access the game information and responses must be displayed on the input device.

The Licensee must ensure that the design of the Lottery System takes into consideration the *World Wide Web Consortium (W3C) standards*, or equivalent, with regards to web interface specifications and online participation requirements.

8   Lottery System Hardware

This chapter sets out the Hardware requirements for Lottery System equipment that must be followed for operation in Victoria.

8.1   Hardware requirements

The design and configuration of all Lottery System equipment Hardware and any changes to Lottery System equipment Hardware must be submitted by the Licensee to the Commission for approval.

The terminal Hardware must provide the means for selling, paying and cancelling entries and other transactions associated with the Authorised Lotteries to be carried out in a manner that is auditable, reliable, secure and fair to Players.

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

8.2   Maintenance requirements

Maintenance of Lottery System equipment is the responsibility of the Licensee. At the discretion of the Licensee, the maintenance may be performed by an approved contracted third party.

Unless otherwise agreed with the Commission, all scheduled maintenance must be carried out in accordance with a maintenance schedule that has been approved by the Commission, along with processes that provide for the security and integrity of work carried out, including appropriate supervision and oversight of work by third parties.

8.2.1   Retention of data

The lottery system must support the licensee's obligations in the Licence and Ancillary Agreement(s) in respect of the retention of data.

To this end, all equipment statistics and lottery information stored in the equipment (whether by electronic, magnetic, mechanical or other means) shall be retained during Hardware maintenance and shall be protected against damage, destruction or alteration during maintenance operations (including battery replacement).

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

8.2.2   Maintenance not to infringe approval

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

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

9 Lottery System Software

This chapter sets out the software requirements for Lottery System equipment.

9.1 Software requirements

Commission approval must be obtained for the design and configuration of all Lottery System equipment software and any changes to Lottery System equipment software used within the Lottery System, including but not limited to Lottery System equipment for Distributors.

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

9.2 Software quality requirements

9.2.1 Software

The components of the Lottery System must be provided to the Tester in an agreed format to enable comprehensive testing. Program and functional documentation must also be provided.

Source code supplied to the Tester (or as agreed) shall be exactly as installed, programmed or loaded in the equipment to be used.

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

- module name
- version
- brief description of functions performed
- edit history: who, why and when (of changes made after this date).

Alternatively, the software identification may be managed by a source code repository platform, provided it can be demonstrated to the satisfaction of the Tester and/or the Commission that such a platform manages the information securely and efficiently and that the information is readily available as required.

9.2.2 Source compilation

The Commission and the Licensee must agree a process to verify that the Lottery System program(s) running are identical to the programs evaluated.

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

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

9.2.3 Source control and upgrade

Approval must be obtained from the Commission for each software revision.

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

Software storage media must be secure, clearly documented and identifiable and must contain all software version control information. The identification used is at the discretion of the Licensee but it must strictly follow the Licensee's identification system as detailed in the software change control procedures.

9.2.4   Software verification during development

The Licensee and/or suppliers of Lottery System software must provide a method to the Commission to enable confidence to be gained that the software on which evaluation was performed, system testing conducted and finally submitted for live operation are directly equivalent. Live operation will not be approved until all steps are in place.

To this end, the following minimum goals are to be met:

- There must be a method available to the Tester for comparing two different versions of the source code and examining the differences between the two versions.
- There must be a method available to verify that the executable software that is to be used for testing has been compiled from the source code versions submitted to the Commission.
- If software changes are required during the testing process all changes must be submitted via the source code. Examination of differences and verification of executable or data files will be undertaken by the Commission or its representatives via receipt of a re-submission of the updated release.
- There must be a method available to verify that the executable software that has been used during the testing process is identical to that which is to operate on the live system. This verification procedure must occur when new software is installed, at the start of each trading day by the Licensee and randomly on demand by the Commission.
- There must be a method available to determine if programs, command files, fixed data files, etc. other than approved baseline elements or identified non-baseline elements reside on any component in the Lottery System.

10 Random Number Generator

This chapter sets out the Random Number Generator requirements that must be followed for operation in Victoria.

10.1 Random Number Generator (RNG)

The Commission requires the use of an appropriate RNG for the selection of the results of Authorised Lotteries. RNG outcomes must not be biased or in any way predictable.

The Licensee must provide and make available to the Commission a tool, a process or software solution to authenticate the software of an electronic RNG.

The Licensee must establish a process for the statistical analysis of Mechanical RNG results for the detection of bias.

Commission approval must be obtained for:

- the RNG algorithm (in the case of an electronic RNG) and its use
- the Mechanical RNG and its procedures (including the adherence to an appropriate maintenance program).

10.1.1 Physically separate electronic RNG unit

If the RNG is a separate, self-contained electronic unit, it must be connected to the central Lottery System computers via an approved communication medium (e.g. serial data communications).

Commission approval must be obtained for the physical security of the electronic RNG.

Depending on the installation environment of the device, the Commission may require that:

- the cage, case or cabinet is electro-magnetically shielded;
- the electronic RNG must comply with specific requirements for electromagnetic interference as detailed in the Australian/New Zealand Gaming Machine National Standard.

The cage, case or cabinet must be constructed of metal, either solid or small grill with said cabinet grounded to building earth.

The cage, case or cabinet must have the facility to fit "destructible seals" and any authorised or unauthorised entry must be detectable.

The cage, case or cabinet must have at least two (2) high security locks, requiring separate keys to allow entry.

All external connections (except mains power) must be fitted with "destructible seals" and disconnection must be detectable.

10.1.2 Logically Separate electronic RNG

If the electronic RNG is to be logically separated from the Lottery System software, its software must be totally independent of the rest of the Lottery System software.

All inner workings of the electronic RNG must not be accessible by any of the other software.

Communication with the Lottery System software must be only through controlled means in the same manner as if it were a physical connection.

Approval for the logical security of the electronic RNG must be obtained from the Commission.

10.1.3 Electronic RNG Software Storage

Commission approval must be obtained for the method of program storage in the electronic RNG and the method(s) for changing the program within the electronic RNG, including appropriate security protection against non-approved changing.

Prior approval must be obtained from the Commission each time the electronic RNG program is to be changed.

10.1.4 Duplicated electronic RNG Units

The electronic RNG units must be duplicated – therefore, there must be at least two electronic RNG's available during normal operation:

- If the electronic RNG is implemented as a physically separate electronic RNG unit, there must be two such units; or
- If the electronic RNG software is contained within the Lottery System's computer network there must be logically separated software in (at least) the back-up computer system(s).

A back-up electronic RNG must be approved, operational and readily available to be swapped in should there be a failure of the primary unit.

10.1.5 Record of Electronic RNG Lottery Selections

When the electronic RNG has selected the required numbers that are the "result" of the Authorised Lottery, these results must be recorded to a permanent storage device in a form that can be authenticated to detect any subsequent modification, before communication of the numbers drawn to the central computer is commenced.

Should there be some kind of failure before the central computer has recorded all of the required numbers, the recorded output may be used to manually complete that draw, in accordance with operational procedures approved by the Commission.

As a minimum, the procedures must require two persons to independently input the results which must then be verified / compared electronically with the RNG outcome.

The recorded output must include, but not limited to, the following information:

- Date
- Time
- The Authorised Lottery name
- The Authorised Lottery draw number
- The numbers/letters drawn (consistent with the Lottery Rules)
- A unique checksum (that is to be entered with the numbers and checked by the Lottery System when manual entry of numbers is required)
- Other security information if available.

The recorded output must be held and be able to be acessed or retrieved for seven years from the date of the draw, for those draws that are held within the term of the Licence.

10.1.6 Mechanical RNG unit

If the RNG is a Mechanical RNG, it must be capable of generating random results consistent with the approved Lottery Rules.

The Commission must be satisfied with the physical security of the Mechanical RNG, including storage.

Each Mechanical RNG must be subject to an appropriate maintenance program (agreed by the Commission) to ensure the device delivers random outcomes, consistent with the Lottery Rules for the Authorised Lottery for which the device is used.

Appropriate operating procedures, agreed by the Commission, must be provided for Mechanical RNG.

The Commission may request the inspection of the RNG and the maintenance program at any given time.

Mechanical RNGs may be tested by a Tester or a qualified person deemed suitable by the Commission.

10.1.7 Duplicated Mechanical RNG Units

A back-up Mechanical RNG unit must be:

- a Commission approved Mechanical RNG device
- must have appropriate procedures, agreed by the Commission, for use as a back-up Mechanical RNG, to determine the outcome of the lottery in accordance with its Lottery Rules
- must be subject to an appropriate maintenance program (agreed to by the Commission) to ensure the device delivers random outcomes, consistent with the Lottery Rules for each lottery for which the device may be used
- must be capable of drawing numbers/letter, etc. as required by the approved Lottery Rules.

10.1.8 Record of Mechanical RNG Lottery Selections

Mechanical RNG results must be recorded to a permanent storage device in a form that can be authenticated, and communicated to the central Lottery System, in a procedure approved by the Commission.

11 Player account requirements

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

11.1 Privacy of Players' personal information

Any information obtained and maintained by the Licensee in respect of a Player accounts must be kept confidential by the Licensee as required under the Licence and Ancillary Agreement(s), except where the release of that information is required by law or approved by the registered Player.

Players' personal data must be managed in accordance with the *Privacy and Data Protection Act 2014(Victoria)* and the *Privacy Act 1988 (Commonwealth)*.

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.

11.2 Maintaining Player account information

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

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

All transactions involving a Player's activity data are to be treated as vital information to be recovered by the Lottery System in the event of a failure.

Personal information of a sensitive nature must only be kept and stored in an encrypted form in transit outside the secure data environment. 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'*.

Personal information of a sensitive nature includes, but is not limited to:

- financial institution account numbers
- credit and debit card numbers, or equivalent
- credit and debit card expiry dates, except where the management of credit card details is PCI compliant
- card security value (CSV) numbers
- expected answers to any questions used to verify a player's identify, e.g. mother's maiden name; and
- balances of Player accounts stored on the Lottery System

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

- a Player's PIN and password used to access details of their Lottery System Player account
- a Player's PIN and password used to access details of their financial institution account.

11.3 Retention of Unclaimed Tickets and Inactive Accounts

The Lottery System must securely maintain a register of all prize tickets that have not been claimed as required by relevant legislation.

The Lottery System must securely maintain a register of all inactive accounts.

The Lottery System shall hold these monies in trust for distribution as required by relevant legislation.

The Commission requires that if there are to be 'old' unclaimed tickets stored on the system, the serial numbers or other access method is to be secured. The method used to secure the information must ensure that a program cannot be run to provide a list of unclaimed tickets that might be obtained and used without authorisation.

Unclaimed ticket information must be removed from the Lottery System after relevant amounts and ticket entry information has been provided to the relevant statutory body in line with unclaimed money requirements.

11.4 Player account statements

The system must be able to make account statements available to the Player upon request.

Account statements must include sufficient information to allow the Player to manage, monitor and assess their gambling activity in relation to Public Lotteries.

12 Network and communications

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

12.1 Communications requirements

12.1.1 Communication scheme

Unless otherwise agreed by the Commission:

- all communications must be via a protocol based communications scheme
- signature verification of all approved Baseline software must be initiated and the outcome verified by a separate, higher-level component of the Lottery System.

12.1.2 Data communications

The Licensee must use appropriate protocol for data communication. This will form part of the Lottery System approval.

Communications protocols must include but not limited to the following:

- error control
- flow control
- link control (remote connection).

Communications protocols must make use of **SIA** process or equivalent.

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

All Lottery System equipment and data must be recoverable to the point of failure following an interruption.

Some typical scenarios to be tested by the Tester to ensure compliance of the system failure and recovery processes are:

- failure of central computer LAN interfaces
- failure of LAN
- failure of data communication interface devices
- failure of single data communication interface
- WAN edge network device failure at central
- WAN edge network device failure at remote
- high data communications error rates on line
- a foreign or additional device placed on a LAN
- a foreign or additional device placed between LAN bridges, communications controllers, or on data communication lines between sites
- single data communication port failure on remote controller (if any)
- LAN failure on regional or local controller (if any)
- data communication interface failure on a lottery device.

12.2 Cryptographic Data Security

12.2.1 Requirement for Cryptographic Data Security

The following requirements must apply to Cryptographic Data Security:

- all Critical Data that traverse data communications lines
- all Critical data transfer between an Agent/Distributors Lottery System equipment and the central site.
- disabling of encryption must only occur with the prior approval of the Commission.

Examples of Critical Data security which would be satisfied by an approved message authentication algorithm include software downloads of any security related software.

12.2.2 Algorithm and Encryption Keys

The Licensee must provide Cryptographic Data Security that meets industry standard encryption and authentication structures. Appropriate encryption must:

- demonstrably secure against cryptanalytic attacks
- employ secure methodology of changing encryption keys
- designed to prevent the creation of an original message from a hash value
- not allow the creation of two messages that hash to the same hash value.

12.3 Network requirements

12.3.1 General

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

12.3.2 Network Baseline

During the approval stage of a system network, and consistent with the System Baseline Document prepared by the Licensee, the Commission will determine the core areas of the system network for which verification control must be maintained.

This document must include an up to date schematic diagram of the Lottery System. The control and security measures of the core systems network is defined and approved in a Network Policy Document.

This document must describe the network topology of the system detailing the interconnection of modules within the core network and the types of connections permitted.

These documents are the responsibility of the Licensee to prepare and maintain as part of its submission to the Commission when obtaining approval for the Lottery System.

12.3.3 Physical requirements

Power to devices inside and on the boundary of the Baseline envelope must be provided from a filtered, dedicated power circuit. This excludes Distribution terminals.

Cabling used in production networks must be of a suitable standard and protected against unauthorised physical access and malicious damage.

12.3.4 Network cabling documentation

All cabling and devices must be clearly labelled by function.

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

12.3.5 Connection of devices to networks inside a Baseline envelope

Unused ports on network devices and network control devices inside and on the boundary of the Baseline envelope are to be disabled.

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

Configuration changes to all devices inside and on the boundary of the Baseline envelope must be password protected. Password protection procedures must exist and be implemented to a standard previously referenced within this document. This provision applies equally to agency and central site networks.

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

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

12.3.6 Communications within a Baseline envelope

Hosts within the same Baseline envelope must be able to communicate during periods of high utilisation, of any and all networks within the envelope, without any significant impact on system performance.

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

12.3.7 Communications between separate Baseline envelopes

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

Hosts within separate Baseline envelopes that communicate with each other must be able to communicate during periods of high utilisation, of any and all networks between the envelopes, without any significant impact on system performance.

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

Communication between devices in separate Baseline envelopes must be immune from 'man-in-the-middle' attacks.

12.3.8 Communications to devices outside a Baseline envelope (Firewall)

Data exchanged with computer systems and terminals outside the Baseline envelope must pass through at least one network control device (for example router or Firewall). The network control devices must implement the controls as defined in the Network Policy Document.

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

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.

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.

Computer systems within the Baseline envelope must be protected (using current best practice) from network attacks (for example ping-of-death attacks, teardrop attacks, routing protocol attacks, denial-of-service, etc.).

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

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:

- authentication scheme
- encryption scheme (encryption must occur at the boundary and inside the Baseline envelope)
- physical security of the external terminal devices and computer systems
- host level security of the external terminal devices and computer systems
- physical security of the network (including intervening hubs, bridges, routers, etc.) to the external devices
- the sensitivity of the information being transferred
- whether the computer system inside the Baseline envelope or outside the Baseline envelope initiates information transfer
- audit information recorded on the Lottery System pertaining to the transfer (date, time, person account or system account, and file(s) transferred)
- immunity from man-in-the-middle attacks.

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

12.3.9 Host monitoring systems and network management systems

Host monitoring systems and network management systems must not enact any change to the system baseline or the network baseline envelope without approval (formal authorisation) from the Commission. Host monitoring systems and network management systems must be tested to verify that they are not capable of enacting any change to the baseline. Verification of the system baseline must be performed at least daily to ensure that unapproved changes have not occurred.

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

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

- imitating the IP address of a host monitoring system or a network management system
- imitating the Hardware address (for example Ethernet address) of a host monitoring system or a network management system, or
- replaying previously captured communications.

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

- imitating the IP address of a host monitoring system or a network management system
- imitating the Hardware address (for example Ethernet address) of a host monitoring system or a network management system, or
- replaying previously captured communications.

12.3.10 Internet connections

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

The Lottery System, at the point where it is connected to the internet service provider, must incorporate secure infrastructure to meet required security standards for the Lottery System.

Design and/or management of the internal and external Firewalls must ensure that any weakness in one Firewall structure is not duplicated in any other Firewall.

The Licensee must have the ability to terminate a remote customer's session.

12.3.11 Verification tools

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

12.4   Wireless communication

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

Wireless communication will be considered for local area network communications within an agency and/or wide area network communication between agencies and the host Lottery System, excluding telecommunication provider's mobile broadband network as critical data communications between agencies and the host Lottery System is encrypted as detailed in section 12.2 *Cryptographic Data Security* of this document.

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

The access point must not be placed directly onto the Agent/Distributor network unless a stand-alone state-full packet inspection Firewall is employed.

Wireless network traffic must be secured with additional encryption and/or authentication codes.

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

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

13 Submission Requirements

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

13.1 General

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

- background of the Lottery System
- purpose of the submission
- description of the scope of system and operational changes
- Tester recommendation of the Lottery System in accordance with above requirements
- the Licensee's comments on any conditions and/or observations included in the Tester report
- list of all software versions and associated SIAs
- list of all relevant Hardware and operating systems – product names, models and versions
- associated systems that are connected to the Lottery System
- an up to date System Baseline document
- Network Policy Document.

13.2 Lottery system operational requirements

The Licensee must have internal controls, rules, policies and procedure manuals or other documents as applicable, which are consistent with this document and other Commission requirements. These documents must be available for the Commission.

The Licensee must provide details of the service management framework for operation of the Lottery System which includes the ICT service management framework.

13.3 Communications

13.3.1 Authentication and encryption

The Licensee must provide details of the message authentication algorithm used.

The Licensee must provide details of the encryption to be used:

- encryption algorithms
- size of encryption keys
- key exchange procedure at session start-up
- subsequent key exchanges
- details of any information that is not encrypted for transmission.

13.3.2 Lottery system internal network architecture

The Licensee must provide details of the proposed architecture of the internal production network to be used to supply Lottery System facilities:

- network topology

- devices used to create the network
- controls to prevent unauthorised modification to device configuration.

The Licensee must provide a description of the details of connections to the Internet.

The Licensee must provide details of any remote connections (for example Internet, WAN, and dial-up) used to support the Public Lottery operations.

The Licensee must provide details of authentication and encryption associated with remote connections.

The Licensee must provide details of Agency terminals, including:

- location of Agency terminals in relation to the Lottery System
- protocols used by Agency terminal connections
- access controls on Agency terminal connections to the Lottery System
- authentication and encryption used by Agency terminals
- controls to prevent eavesdropping on communications between Agency terminals and the Lottery System
- controls to prevent unauthorised use of Agency terminals.

The Licensee must provide a list of all non-Baseline systems that will connect to the Lottery System.

For each non-Baseline system, the Licensee must provide:

- the connection method
- details of the information to be transferred in each direction
- the entity that initiates the information transfer
- the protocol used to perform the transfer
- the controls in place to prevent access to other information on the Lottery System
- the controls in place to prevent unauthorised use of the connection
- the controls in place to prevent eavesdropping on communications pathways.

The Licensee must provide details and configurations of the devices that will be used to control access from the Internet to the Baseline network (including authentication and encryption).

The Licensee must provide details and configurations of the devices that will be used to control access from other networks (including non-Baseline networks used by the Licensee) to the Baseline network.

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

The Licensee must provide details of any network management system associated with the Baseline network, including the:

- physical location of the network management system
- class of personnel authorised to use network management system
- locations from where network management functions can be executed
- network management protocol
- devices to be managed on a read only basis
- devices to be managed on a read/write basis
- controls in place to prevent unauthorised access to network management functions
- controls in place to audit the use of network management functions
- controls in place to detect unauthorised connections to the network
- controls in place to detect connection of unauthorised equipment to the network.

The Licensee must provide descriptions of the locations and physical and logical security arrangements associated with domain name servers within the Baseline network.

13.3.3 Lottery system computers

The Licensee must provide an overview of the Lottery System design, including a detailed design document(s) and a functional specification.

The Licensee must provide details of all computer systems used by the Lottery System including, but not limited to:

- Hardware platform
- operating system
- applications
- audit subsystem
- duplication strategy
- disk subsystem
- back-up facilities
- physical security
- login security
- power requirements
- environmental condition requirements.

The information requested above also applies to other Lottery System equipment to be used in the Lottery System computer environment. This includes, but not limited to, such devices as:

- front ends
- Firewalls
- operator consoles (local and remote)
- remote controllers
- remote access servers
- multiplexing equipment
- switching equipment
- monitoring equipment
- routers
- any other applicable appliances.

For each Lottery System component and associated equipment that is to be implemented, the Licensee must provide a detailed schedule of the planned implementation.

In relation to the Lottery System, the Licensee must provide:

- details of statistics that are stored by the system
- detailed descriptions of its password protection systems and associated algorithms utilised by the system
- description of the method of transaction logging used
- explanations of the situations during which encryption of data files will be employed
- where data files encryption is to be employed:
  - description of the algorithm
  - theoretical basis of the algorithm
  - results of any analyses or tests to demonstrate that the algorithm is suitable for the intended application

- o   rules for selection of keys
    - o   means of setting and protecting keys
- description on how self-monitoring is to be implemented.

13.3.4 Lottery system software

The Licensee must provide the source software for Lottery System software, as agreed to by the Commission.

The Licensee must provide a description of the method to be used to verify the integrity of the software operating on the production Lottery System.

13.3.5 Lottery system operations

The Licensee must provide details of each class of account required to operate the Lottery System in a Baseline environment (for example system administrator, operator, hotline, network support).

For each class of account provided the Licensee must provide details of the privileges required to perform the duties associated with that account.

The Licensee must provide details of the physical location of each component of the Lottery System, including the location of staff.

The Licensee must provide Lottery System operators manuals, operator's procedures manuals and system administrator manuals or equivalent.

The Licensee must provide copies of all standard reports produced by the Lottery System and describe how these are generated.

14 Testing requirements

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

14.1 Inspection and testing

The Commission may have regard to a recommendation for system approval from a Tester listed on the Roll.

The Licensee must establish and maintain policies, procedures and standards for quality assurance and control equivalent to ISO/IEC 27001:2013, and a test strategy that must be available to the Tester. These include, but are not limited to:

- network Hardware and communications infrastructure
- system functionality
- system interfaces
- usability, including ease of use for customer facing devices and Graphical User Interfaces (GUI)
- accessibility, including but not limited to assessing against World Wide Web Consortium (W3C) standards, or equivalent
- user acceptance
- performance, including but not limited to load generation for response, stress, volume and soak testing of system, database and network configurations
- security, including but not limited to testing system and network configurations for vulnerability, penetration, hacking, cracking, virus, spy ware, spam or denial-of-service attacks
- disaster recovery
- system backup and recovery
- business readiness, including provision for a live trial when required by the Commission.

The Licensee's test strategy must identify any independent or third party testing, including internal and external test facilities, and the engagement mechanism for working with a Tester.

14.1.1 Tester evaluation

The Tester will work with the Licensee to undertake the evaluation of the Lottery System to ensure it meets the requirements set out in the Licence and Ancillary Agreement(s) any other relevant standards, specifications or conditions determined by the Commission.

Should the Tester's evaluation be deemed inadequate by the Commission, such as sole reliance on paper based testing, further evidence or testing will be required.

The Tester will provide a report to the Commission in consideration of the system's:

- integrity and reliability
- compliance with all the legislative, technical, and reporting requirements
- security and controls
- policies and procedures
- Baseline and network security policy document.

14.1.2 Facilities for a Tester

The Licensee must make the appropriate facilities available to a Tester in the course of the Licensee's engagement of a Tester in order that a Tester is in a position to conduct an adequate evaluation of the system (or changes to an approved the system) and make its recommendation to the Commission.

14.1.3 Resources for a Tester

The Licensee must provide the appropriate resources (technical, administrative) to assist the Tester in completion of tasks.

14.1.4 Test environment

The Licensee must ensure that upgrades to the Lottery System and associated Lottery System equipment can be adequately tested in an appropriate test environment using a test system that is functionally, not necessarily physically, identical to that proposed for use in production.

The test system must not share the Baseline system.

There must be a method to verify that the Baseline software evaluated and recommended for approval (by a Tester) on the test system is the same Baseline software that has been migrated to the production system following the Baseline software's approval.

14.1.5 Failure modes and recovery testing

The Licensee must ensure that a Tester is able to test the host Lottery System for resilience, recoverability and continuity of service, including but not limited to conditions for:

- failure of host Lottery System power supply
- total power failure of the host Lottery System site
- verifying there is no single point of failure
- individual server capability to sustain persistent load
- guaranteed messaging
- failure of critical components, including but not limited to processors, handlers, gateways, API's, and communication protocols or similar
- failure of critical storage devices, including those holding data files and databases critical to the operation
- failure of host Lottery System I/O Channels
- failure of links with remote interface points
- host Lottery System operator error, including but not limited to invalid data entry
- daylight savings changeover.

14.2 System testing requirements

14.2.1 Testing requirements and Tester recommendation

The security and controls, functional specifications, and all the requirements of the system are to be evaluated and recommended by a Tester.

A Tester recommendation is required on:

- integrity and reliability
- compliance with all the legislative, technical, and reporting requirements

- security and controls
- policies and procedures
- Baseline and network security policy document.

14.2.2 Associated systems requirements

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

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

15 Document Information

15.1 Document Details

CRITERIA	DETAILS
Document title:	Victorian Lottery System Requirements document
Document owner	Victorian Gambling and Casino Control Commission

15.2 Approvals

NAME	POSITION	FUNCTION
Commission	The VGCCC Commission or delegate (CEO)	Approve

16 Reference Material

Australian Government Information and Communications Technology Security Manual (ISM) – Controls, as amended from time to time http://www.asd.gov.au/publications/Information_Security_Manual_2015_Controls.pdf, viewed at 1 December 2015.

Victorian Government Website Management Framework – Accessibility standard', as amended from time to time - available from Enterprise Solutions Victoria

'SEC GUIDE 03 Information security penetration testing guideline', as amended from time to time – available from Enterprise Solutions Victoria, last viewed December 2015.

Related online and mobile guidelines - http://www.enterprisesolutions.vic.gov.au/business-systems/online-and-mobile/, viewed at 1 December 2015

World Wide Web Consortium (W3C) Standards, or equivalent

World Lottery Association WLA Security Control Standard

17 Appendix A – Emergency Change Documentation

This Appendix sets out the document that must be submitted to the Commission after emergency changes to the Lottery System.

17.1.1 Emergency Change Request Form

To:	Manager, Licence Management & Audit
	Senior Auditor, Licence Management & Audit
	Evaluation Officer, Licence Management & Audit
Internal Distribution List	

Reference Number	
Prepared By	
Signature	
Date/Time	
Prepared By	
Signature	
Date/Time	
Authorised By	
Signature	
Date/Time	

IMPACTS (System, Player, Data, Gambling Integrity, Security, etc.):

INCIDENT (description of & justification for the change):

RESOLUTION

CRC VERIFICATION GLOBAL BASELINE

Old Global CRC	
New Global CRC	

CRC VERIFICATION AFFECTED FILES

Affected File Name	Old CRC	
	New CRC	
Affected File Name	Old CRC	
	New CRC	
Affected File Name	Old CRC	
	New CRC	

VGCCC CONTACT INFORMATION

Name of Officer contacted	
Officer contacted verbally	Yes/No
Voicemail message	Yes/No
Date/Time of contact	