# Table of Contents

## 1 INTRODUCTION

- General .......................................................................................................................... 3
- *Introduction* .................................................................................................................. 3
- *The Act* ....................................................................................................................... 3
- *Objectives* ..................................................................................................................... 3

- Approved Lottery Equipment .................................................................................... 4
- *Provision of Information* ........................................................................................... 4
- *Approval of Lottery Equipment* .................................................................................. 4
- *Inspection of Delivered Lottery Equipment* ............................................................... 4
- *Equipment Operation - Special Dispensation* ............................................................ 4

## 2 CENTRAL SYSTEM REQUIREMENTS

- Central System Environment ....................................................................................... 5
- *Central System Accommodation* ............................................................................... 5

- Central System Host - General ..................................................................................... 6
  - *Central System Software Procedures* ......................................................................... 6
  - *System Baseline* ......................................................................................................... 7
  - *Software Quality* ......................................................................................................... 8
  - *Central Logging of Information* ................................................................................... 8
  - *Generation of Significant Events* ............................................................................... 9
  - *Retention of Unclaimed Moneys and Dormant Accounts* ........................................... 9

- Central System Security & Recovery ........................................................................... 9
  - *System Audit* .............................................................................................................. 10
  - *Access by Commission* ............................................................................................ 10
  - *Central System Recovery* ........................................................................................... 11
  - *Data Security* .............................................................................................................. 12

- Central System Integrity .............................................................................................. 12
  - *Multiple Data Files* ..................................................................................................... 12
  - *Data and Event Collection* ........................................................................................ 12
  - *Commission Required Reports* .................................................................................. 12
  - *Central System Integration* ....................................................................................... 13
  - *Link to Commission Computing Facilities* ............................................................... 13
  - *Inspection and Testing* ............................................................................................... 13

## 3 NETWORK AND COMMUNICATIONS

- Communications Requirements ................................................................................... 14
  - *Requirements for Encryption* .................................................................................... 14

- Network Requirements ............................................................................................... 15
  - *Network Topology* .................................................................................................... 15
  - *Internet Connections* ............................................................................................... 17
  - *Verification tools* ....................................................................................................... 18

## 4 SYSTEM TESTING REQUIREMENTS

- Testing Requirements and Tester’s Certificate ............................................................ 19
- Associated Systems Requirements ............................................................................... 19
- Submissions Requirements ......................................................................................... 19
1 Introduction

This chapter introduces the concept and the purpose of the Lottery System Document.

1.1 General

Introduction

1.1.1 The Lottery System Document contains the system related technical requirements for a lottery system operating in Victoria.

1.1.2 This document will be used by an Accredited Testing Facility (ATF) to evaluate a system against when an operator submits the system for approval.

1.1.3 Other system operational requirements such as system audit, revenue audit, system verification and recovery are also defined in this document.

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

1.1.5 All references in this document pertaining to the Victorian Commission for Gambling Regulation (referred to as ‘the Commission’) include its staff.

1.1.6 This document replaces and supersedes the Footy Tipping Systems Document Version 1.0.

The Act

1.1.7 The requirements specified in this document are supplementary to and do not take the place of any of the requirements of the Gambling Regulation Act 2003 (referred to as ‘the Act’) or the Public Lotteries Licence conditions (if any).

Objectives

1.1.8 The Commission is looking to set high systems integrity standards for lottery equipment operating in Victoria for the purpose of ensuring that:

a) the system operates in accordance with the rules of the competition;

b) the system is fair to players;

c) the system operates in a manner that is auditable, reliable and secure; and

d) all parties receive the correct entitlement for lottery subscriptions and revenue.
Lottery System Document

1.1.9 Matters arising from the testing of lottery equipment which have not been addressed in this document (due to omissions or new technology) will be resolved at the sole discretion of the Commission as part of the approval process.

1.2 Approved Lottery Equipment

Provision of Information

1.1.10 The Commission may require information on any current equipment in operation.

1.1.11 An operator must maintain and retain all records pertaining to the design, manufacture and testing of software and equipment which may be required by the Commission.

1.1.12 When evaluating the system(s) for approval, the operator must provide sufficient information and documentation to an ATF to enable a full determination of the system’s level of compliance with this requirements document.

Approval of Lottery Equipment

1.1.13 Only approved lottery equipment may be operated in Victoria. Contact the Commission regarding the process to submit equipment for testing and approval.

Inspection of Delivered Lottery Equipment

1.1.14 The Commission may inspect delivered equipment in the field (or at the host site) and reject any equipment that is not approved.

Equipment Operation - Special Dispensation

1.1.15 In special circumstances, lottery equipment, which does not fully comply with all requirements specified in this document, may be considered for approval provided adequate compensating controls are in place.

1.2.7 The granting of “special dispensation” will be at the sole discretion of the Commission.
2

Central System Requirements

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

2.1 Central System Environment

2.1.1 The Commission requires that the lottery operator implement a computerised Central System capable of meeting the following broad functions:

a) ability to support the requirements of the Act and Public Lottery Licence conditions (if any);
b) ability to support the rules of the competition;
c) ability to support the predicted system load requirements;
d) ability to provide adequate system audit and security requirements;
e) ability to provide adequate financial verification and audit capabilities;
f) ability to provide reports as required by the Commission.

2.1.2 The Central System must be a computer-based system with sufficient capacity (processing, memory, communications interfaces and hard disk storage) to efficiently perform all tasks associated with providing a lottery competition.

2.1.3 An electronic lottery system is deemed to extend to the point at which the competition is offered to the players.

Central System Accommodation

Physical Security

2.1.4 The Central System computer room(s) is to be a secure area where only authorised personnel may enter. The Commission requires the adoption of an electronic locking system that provides monitoring information on the entry/exit of personnel.

2.1.5 Procedures are to be maintained to ensure only authorised personnel are given access, and there is to be a detection system that provides an alarm when unauthorised entry to the computer room is attempted.

Emergency Lighting

2.1.6
Environment Monitoring System

2.1.7 Power Supply

2.1.8 All Central System equipment and powered devices (lights, air conditioning, telephone, etc.) within or contributing to the computer room(s) environment must be supported by at least one UPS and at least one stand-by generator.

2.1.9 The computer systems must be protected against power fluctuations and temporary loss by installation of an UPS or other such device.

2.1.10 The UPS must provide sufficient supply to support the Central System until the generator is started, and enable the systems to be shut down in an orderly manner without the loss of data, should the generators fail.

2.1.11 All equipment situated in the computer room is to be earthed through the UPS.

2.1.12 UPS, generator, emergency lighting and other such systems referred to herein must be tested at least every three months.

2.1.13 Testing of these procedures and facilities are to be logged, and the logbook is to be available for inspection by the Commission. The Commission may request to be in attendance at any test.

2.1.14 Hotline terminal(s) and lighting are to be supported by the back-up power system.

2.1.15 The Central System is to be protected against long-term loss of power by the installation of a generator or other such device. The generator must have the fuel capacity to support the computer systems, air conditioning, security system, telecommunication equipment, computer terminals and sufficient lighting for normal operation of the Central System equipment for a period of not less than 24 hours.

Hot-Line Telephone System

2.1.16 If the lottery network consists of one or more remote sites, a “Hotline” or “Help Desk” facility is to be provided to assist participating outlets with problems, disputes and maintenance calls.

2.1.17 The Hotline telephone system is to enable direct access to multiple operators via a call to a dedicated telephone number that is not routed via the operator’s switchboard. There should be sufficient capacity on this dedicated number for normal operation.

2.2 Central System Host – General

2.2.1 The lottery system must operate in accordance with the approved rules of the competition.

2.2.2 The Commission will approve the software configuration (baseline) of the Central System host.

2.2.3 An ATF will evaluate the lottery system software and hardware configuration for reliability, recovery, auditability, redundancy, and security.

Central System Software Procedures

2.2.4 The lottery operator is to have in place procedures for virus protection and detection, where a material risk of virus infection exists.
Lottery System Document

2.2.5 The operational control of the Central System must be administered in accordance with relevant internal control procedures.

2.2.6 Only approved application files may reside on disk or in the memory of the host Central System computers.

System Baseline

2.2.7 The approved lotteries system will be subject to a condition that the operator must not access and undertake any changes to the system baseline without the approval by the Commission or its delegate.

2.2.8 The system baseline is to consist of system software and hardware components and network and communication that enable the system to operate in a secure environment and meet the legislative requirements.

2.2.9 The operator must document all of system components and identify those that are core to the system operations to be submitted as part of the request for system approval.

2.2.10 The following are considered to be in the system baseline document:

i) All the system components which represent the core components of the lottery system must be included in the baseline document. Any changes to those components including the emergency changes are subject to approval by the Commission having regard to tester’s certificate;

ii) Application files such as those associated with allocating entries tickets to a particular draw number, secure “Closed” pool environment and allocate ticket entries to the next draw after the draw “Closed”;

iii) Application files associated with products where the results of which are continuing for the whole season (eg Instant tickets, footy tipping etc);

iv) operating systems which provide secure environment;

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

vi) central systems communication devices that interface with any outlet equipment;

vii) the method used to verify that the system is operating in an approved state;

viii) a system network document, which clearly identifies the core areas of the system network. This document should describe the network topology of the system, detailing the interconnection of modules within the network, and the type of connection between the modules that is permitted;

ix) any other operations or procedures issues that are relevant to the securing control of the system;

2.2.11 Tester’s certification is required for all changes to the system baseline document;

2.2.12 There is a requirement for an agreement to be reached relating to the directories in which application files will be located on the Central System computers in order to establish a baseline document. Files which cannot be verified because they change frequently are not expected to be stored in system application directories.
Lottery System Document

2.2.13 The Commission requires that the Central System have some method to verify the system application executable files (and selected command utilities) in order to confirm that the configuration of the system is operating in an approved state.

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

Software Quality

Software Version Control

2.2.15 All software for all components of the Central System must be maintained under an appropriate software version control system or mechanism.

Software Verification During Development

2.2.16 The lottery operator and/or its suppliers must ensure there is a method in place for the software on which the ATF evaluation was performed is the same as the software submitted for approval and live operation. To this end the following goals are to be met:

a) all system baseline files and other software files that operate the lottery system are to be made available (to an ATF) in machine-readable form.

b) a procedure which outlines the method for examining the source code and conducting computer-aided searches.

c) a procedure which outlines the method for comparing two different versions of the source code and examining the differences between the two versions.

d) the ATF must verify and confirm that all the system software being submitted for approval are the same as that which was evaluated. Only the system baseline files are required to be included with the submission approval.

e) if software changes are required during the integration testing process, all changes must be submitted via the source software. Examination of differences and verification of executable or data files may be undertaken by the Commission by compiling the submitted source code.

f) a procedure which outlines the method for verifying that the executable software on the production system is operating in an approved state.

g) a procedure which outlines the method for detecting unapproved programs, command files, fixed data files, etc. that reside on any modules in the lottery system.

Central Logging of Information

2.2.17 All in place security logs must be reviewed and followed-up by the operator in a timely manner.

2.2.18 All accounting and any security event data must be held and be able to be accessed or retrieved (from back-up) for:

a) Significant events - at least 2 years,

b) Financial data - at least 7 years.
Generation of Significant Events

2.2.19 There must be a facility provided by the lottery operator whereby significant events will be reported to the Commission in a format to be determined by the Commission. Typical significant events to be reported on are as follows:

a) situations where the system is incapable of supporting the rules;
b) significant system failures;
c) instances where Internal Control Procedures were unable to be followed;
d) situations where system hardware or software version roll-backs were carried out;
e) instances where significant work-arounds were carried out by the operator;
f) instances where a system verification test result came out incorrect;
g) instances where late closures were identified; and
h) instances where incorrect dividends were identified.

Retention of Unclaimed Moneys and Dormant Accounts

2.2.20 The lottery operator must securely maintain a register of all prize money that has not been claimed as required by relevant legislation.

2.2.21 The lottery operator must securely maintain a register of all dormant accounts (no activity for over a year).

2.2.22 The lottery operator shall hold these monies in trust for distribution as required by relevant legislation.

2.2.23 The Commission requires that if there are to be “old” unclaimed monies stored on the system (unclaimed cash tickets), 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 monies that might be obtained and used without authorisation.

2.2.24

2.3 Central System Security & Recovery

2.3.1 The Commission requires adequate security over the approved system to ensure continued system integrity and auditability.

2.3.2 The operating system of the computer’s gaming application files and database (if applicable) must provide comprehensive password security. The Commission requires that password security includes the following:

a) initial password change on its first use must be enforced;
b) an appropriate minimum password length policy must be enforced;
c) an appropriate methodology for the enforced frequency of password changes must be in place;
d) procedures for password checking against a list of invalid names (dictionary checking) must be in place; and

e) procedures for adequate protection of emergency passwords must be in place.
Lottery System Document

2.3.3 The Commission requires that formal internal reporting and follow-up procedures exist for security breaches. For example:
   a) unauthorised attempts to access a system (sign-on);
   b) unauthorised attempts to access system resources; and
   c) unauthorised attempts to view or change system security definitions or rules.

2.3.4 The Commission requires that there be adequate security policies and configuration management procedures in place relating to any media library administration (and any off-site storage) of data. It is expected that all programs and important data files are only to be accessed by the entry of a password that will be known only to authorised personnel.

2.3.5 The Commission requires that storage of passwords be in an encrypted, non-reversible form.

2.3.6 A program must be available that will list all registered users on the system including their privilege level and this list must be kept current.

System Audit

2.3.7 It is expected that the operator will implement (and maintain) the following matters in regards to system audit:
   a) ensure that adequate system security procedures and policies are in place (and that critical issues are actioned upon by management in a timely and accurate manner);
   b) all significant audit logs must be monitored and followed up;
   c) there must be satisfactory security and control over database applications, and critical configurable parameters to ensure the integrity of the system;
   d) there is to be a method to verify the integrity of the software on the host and any associated peripheral equipment operating in the production environment;
   e) all data editors are to be removed from the system;
   f) all applicable user accesses should be restricted via menu options;
   g) all dial-in access should be strictly monitored and any relevant security related logs are to be followed up in a timely manner;
   h) network and communications security procedures are to be established, enforced and maintained;
   i) all interfaces to any subsystems are to be managed securely, and security reviews are to be performed from time to time;
   j) preventive and detective control measures must be established with respect to the security of the production Central System environment;
   k) the operator must ensure that adequate software change control procedures exist inline with change management processes; and
   l) the Commission requires that adequate emergency change control procedures are in place.

Access by Commission

2.3.8 The operator, at the direction of an authorised Commission officer must provide access to the information on the Central System application and database at any time.
2.3.9

2.3.10 The Central System software is to provide tools and mechanisms to:
   a) examine significant critical events;
   b) examine data; and
   c) verify the approved system baseline.

Central System Recovery

2.3.11

Transaction Logging
2.3.12 A current log of transactions since the last backup is to be maintained at a back-up site.
2.3.13 For transaction logging the Commission requires that:
   a) the Central System is to record (with time/date stamp) all vital transactions received from equipment that processes lottery wagers;
   b) the log file(s) and/or database must be duplicated for integrity and reliability;
   c) the method of transaction logging will be assessed prior to approval; and
   d) all adjustments or modification to the wagers (and unclaimed monies or accounts) must be recorded with the computer operator’s ID (and time/date-stamp).

Disaster Backup & Recovery
2.3.14 In the event of a disaster (for example, a fire) there must be a method of ensuring that data related to player entitlements and government revenue (since the last backup and the transaction log) can be rebuilt up to the point of the disaster.
2.3.15
2.3.16 Copies of all daily database backups must be retained at a location other than the primary site.
2.3.17 There must be periodic back-ups (at least daily) of the variable database files on the Central System’s disks.

System Data Recovery
2.3.18 The Commission requires that, in the event of a failure whereby the system cannot be restarted in any other way, it must be possible to reload the database from the last backup point (the previous night) and fully recover vital transactions via the transaction log up to the point of the failure.
2.3.19 Certain database update information of a non-critical nature may not be required to be automatically recovered. Exceptions of this nature would need first to be agreed with the Commission.
2.3.20 The method used to backup and retrieve the information must ensure that the information is secure and cannot be used or obtained in an unauthorised manner.
Lottery System Document

Data Security

Encryption of Stored Data

2.3.21 The Commission requires, as a minimum, that the following information will be encrypted in a non-reversible form for storage and use:
   a) PINs;
   b) passwords.

2.3.22 The Commission requires as a minimum, that the following information will be encrypted (reversible) for storage or recovery purposes:
   a) encryption/decryption keys; and
   b) unclaimed monies.

PIN Management

2.3.23 If player (or attendant staff) PIN numbers are used in support of the system, the PIN number creation algorithm, its implementation and operational procedures (pertaining to PIN changes, database storage, security and distribution) must be evaluated prior to approval by the Commission.

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

2.4 Central System Integrity

2.4.1 The Commission will approve the hardware configuration of a Central System.

2.4.2 The ATF will evaluate the hardware configuration for reliability, recovery, auditability, redundancy and security.

Multiple Data Files

2.4.3 The Commission requires that electronic memory data files (and/or electronic database files) that contain vital information must be duplicated for integrity and reliability.

Data and Event Collection

2.4.4 Commission Required Reports

2.4.5 As a minimum the following financial information by Lottery draw conducted needs to be made available to the Commission in a format required. The information may be required to be remitted to the Commission in either a hardcopy or text format and/or in an electronic format compatible for processing into Commission’s systems.
   a) total sales by draw
   b) sub total sales (break-up by product)
   c) sub total by state & overseas jurisdictions
   d) player loss by draw, by state & overseas jurisdiction
   e) declared dividends by draw
   f) all jackpot reports by draw
   g) all revenue and tax reports by draw
   h) financial alteration reports showing any amounts changed (and/who/when performed the changes)
   i) cancellation of bets reports showing any bets changed (and who/when performed the changes)
   j) Real time game closure/snap reports for audit to perform game closure verification.
   k) System dividend share reports.
2.4.6

2.4.7 Reports supplied to the Commission must be accurate, clearly printed, and available in electronic format if required.

Central System Integration

2.4.8 The Commission may approve the integration of all sub-systems into the Central System. For example, this could be systems performance monitoring software, added security systems, or any other application, which is assisting in the efficient operation of the system.

2.4.9 The Commission may not approve any information flowing to or from the Central System to subsystems unless the interface is approved and is baselined.

Link to Commission Computing Facilities

2.4.10 There is to be an electronic link from the lottery operator’s Central System site to the Commission’s computer facilities.

2.4.11 This link is for the purpose of downloading financial data on a daily basis (or at a frequency agreed by the Commission) those reports specified in the section “Commission Required Reports”.

Inspection and Testing

Facilities For Inspectors

2.4.12 The Commission may require that for the life of the product, there is to be a securable office facility to assist in the conduct of the Inspector’s duties as necessary for monitoring the lottery system configuration.

Facilities For an ATF

2.4.13

Test System

2.4.14 The lottery operator must ensure that upgrades to the Central System and associated lottery equipment can be adequately tested in an appropriate test environment using a test system.
The test system is not to share any hardware with the production system, except for a power source and other items of hardware for which express permission for exclusion must be sought from the Commission.

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

Central System Failure Modes and Recovery Testing

Some typical tests that must be implemented by an ATF to test compliance with this and other sections of the Central System are:

a) failure of central processor;
b) failure of central computer power supply;
c) failure of central computer memory;
d) failure of central computer disk(s);
e) failure of central computer I/O channels;
f) total power failure of the central site for a short period, (30 seconds);
g) total power failure of the central site for a long period, (30 minutes); and
h) operator error (invalid data entry, etc.).
3

Network and Communications

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

3.1 Communications Requirements

Requirements for Encryption

3.1.1 The following requirements related to encryption apply:

a) The Commission may require that encryption of critical messages that traverse data communications lines be implemented (but not necessarily within the Central System site).

b) Examples of critical messages include:

i. ticket serial numbers;

ii. RNG seeds;

iii. signature seeds (algorithm coefficients);

iv. signature results;

v. encryption keys (where the implementation chosen requires transmission of keys);

vi. PINs;

vii. passwords;

viii. software uploads and downloads of any security related software; and

ix. transfer of money between computer equipment.

c) If encryption is utilised, the Commission requires that there be a password protected (and secure) function to disable encryption to handle circumstances where difficulty with communications is encountered. Disabling of encryption may only occur with the prior approval of the Commission.

Encryption Algorithm Approval

3.1.2 The encryption algorithm, its implementation and operational procedures must all be approved by the Commission. The following are encryption characteristics that will be considered:

a) encryption algorithms are to be demonstrably secure against cryptanalytic attacks; and
there must be a secure method implemented for changing the current encryption key set. It is not acceptable to only use the current key set to “encrypt” the next set. An example of an acceptable method of exchanging keys is the use of public key encryption techniques to transfer new key sets.

**Communication Failure Modes and Recovery**

3.1.3 All lottery equipment must be able to adequately handle a range of simple failures. For example, some typical tests which must, at a minimum be implemented by an ATF to test compliance with this document are:

a) failure of central computer LAN interfaces;
b) failure of central LAN;
c) failure of central data communication interface devices;
d) failure of single data communication interface;
e) high data communications error rates on line;
f) a foreign or additional device placed on a LAN;
g) a foreign or additional device placed between LAN bridges, communications controllers or on data communication lines between sites;
h) single data communication port failure on Remote Controller (if any);
i) LAN failure on Regional or Local Controller (if any); and
j) hosts attached to broadcast networks must recover from broadcast storms that flood the network to 100% utilisation for a period of up to 30 minutes without losing any critical information.

**3.2 Network Requirements**

**Network Topology**

3.2.1 This section describes the Commission’s network requirements on system firewalls, network connections that are inside a baseline envelope (the core area defined by the Commission as to be under baseline control), and network connections from the baseline envelope to external devices.

**Network Baseline**

3.2.2 During the approval stage of a system network, the Commission will determine the core areas of the system network over which verification control must be maintained, and this will be defined and approved in a Network Policy Document. This document is essentially a matrix that describes the network topology of the system, details the interconnection of modules within the network, and the type of connection between the modules that is permitted.

**Physical Requirements**

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

3.2.4 Cabling used in production networks should be protected against unauthorised physical access and malicious damage.

**Network Documentation**

3.2.5 All cabling and devices should be clearly labelled by function.

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

**Connection of External Devices to Networks Inside a Baseline Envelope**

3.2.7 Unused ports on network devices and network control devices inside (and on the boundary) of the baseline envelope are to be disabled.
3.2.8 Host computer systems, network devices and network control devices inside and on the boundary of the baseline envelope must be immune from high loads (broadcast storms) or faults on any part of the network outside the baseline envelope.

3.2.9 Configuration changes to all devices inside and on the boundary of the baseline envelope must be password protected. Password protection procedures must exist and be implemented.

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

3.2.11 At a Central System site, all network devices, network control devices and hosts associated with a production network must be located inside an area that only persons with a valid security clearance can enter.

**Communications Within a Baseline Envelope**

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

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

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

**Communications Between Separate Baseline Envelopes**

3.2.15 Information flowing between different baseline envelopes may be subject to authentication and encryption, unless the intervening network is physically secure and under the complete control of the operator. Note that WAN communication links will be generally deemed to be outside a baseline envelope.

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

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

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

3.2.19 Communication between devices in separate baseline envelopes should be immune from computer/network attacks.

**Communications to Devices Outside a Baseline Envelope (Firewall)**

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

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

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

3.2.23 Network control devices must be configured to discard all traffic other than that, which is specifically permitted by the Network Policy Document. Configurations that discard specific traffic types and allow everything else are not acceptable.
3.2.24 Computer Systems within the baseline envelope must not be affected by computer/network attacks emanating from outside the baseline envelope.

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

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

1. the message authentication scheme utilised;
2. encryption scheme - encryption should occur at the boundary inside the baseline envelope;
3. physical security of the external terminal devices and computer systems;
4. host level security of the external terminal devices and computer systems;
5. physical security of the network (including intervening hubs, bridges and routers) connections to the external devices;
6. the sensitivity of the information being transferred;
7. whether the computer system inside the baseline envelope or outside the baseline envelope initiates information transfer;
8. audit information recorded on the Central System pertaining to the transfer of files and information; and
9. intrusion detection utilised and immunity from computer attacks.

3.2.27 Note that WAN communication links will be generally be deemed to be outside the baseline envelope approved by the Commission.

Computer Monitoring Systems and Network Management Systems

3.2.28 Computer monitoring systems that monitor hosts inside or on the boundary of a baseline envelope must be approved by the Commission.

3.2.29 Network monitoring systems that monitor network devices and network control devices inside or on the boundary of a baseline envelope must be approved by the Commission.

3.2.30 The configuration of Central System monitoring tools and network management systems must not be changed without formal authorisation. Automatic verification of the configuration of these systems must be performed at least weekly.

3.2.31 A device outside a baseline envelope must not be able to affect the configuration of network devices or network control devices by:

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

b) imitating the hardware address (ethernet address) of a host monitoring system or a network management system; or

c) replaying previously captured communications.

3.2.32 A device outside a baseline envelope must not be able to affect the operation of the Central Site or be able to read or modify critical data by:

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

b) imitating the hardware address (ethernet address) of a host monitoring system or a network management system; or

c) replaying previously captured communications.

Internet Connections

3.2.33 Internet connections must demonstrate adequate networked based and host based intrusion detection capabilities. This includes the automatic raising of computer operator alarms in the event that a security breach occurs.
The lottery system at the point where it is connected to the internet service provider must incorporate a DMZ like architecture.

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

The operator must have the ability to terminate a player’s session.

**Verification tools**

The Commission must upon request be provided with sufficient tools and/or procedures to verify the configuration of all devices inside and on the boundary of the baseline envelope approved by the Commission.
This chapter sets out the lottery system testing requirements that must be followed for operation in Victoria

4. SYSTEM TESTING REQUIREMENTS

4.1 TESTING REQUIREMENTS AND TESTER’S CERTIFICATE

4.1.1 The security and controls, functional specifications, and all the above requirements of the system are to be evaluated and tested by a tester listed on the Roll. A tester’s certificate is required on:
   i) the system integrity and reliability
   ii) whether the system meets all the legislative, technical, and reporting requirements
   iii) whether the controls and procedures required exist and are effective
   iv) system baseline for future approval

4.2 ASSOCIATED SYSTEMS REQUIREMENTS

4.2.1 All the systems associated with the lotteries system require to be tested for reliability in processing and delivering all transactions for the lotteries system.

4.2.2 There must be adequate security arrangements and controls between the approved lotteries system and the associated systems. That must form part of the independent assessment and tester’s certification.

4.3 SUBMISSIONS REQUIREMENTS

4.3.1 The submission to the Commission for approval, at the minimum, should include the following:
   i) Background of the system;
   ii) System flow chart in a summary format;
   iii) Independent report on security and controls;
   iv) Tester’s certificate of the lotteries system in accordance with above requirements;
   v) Associated systems that are connected to the lotteries system;
   vi) A System Baseline Document as defined in the above section;