Victoria Government Gazette

No. S 386 Monday 28 November 2011
By Authority of Victorian Government Printer

Gambling Regulation Act 2003 Section 10.1.5A

VICTORIAN COMMISSION FOR GAMBLING REGULATION

Notice of the Amendment of a Standard

Technical Equipment and Systems for a Keno System in Victoria

In accordance with section 10.1.5A(2)(b) of the **Gambling Regulation Act 2003**, the Victorian Commission for Gambling Regulation gives notice that, with the approval of the Minister for Gaming, it has amended a Standard in respect of technical equipment and systems for a Keno system in Victoria.

The amended Standard is Keno Technical Standard Version 1.1.

The Standard comes into force on the date of this notice.

The Standard is published on the Commission's website at www.vcgr.vic.gov.au.

Dated 23 November 2011

JANE BROCKINGTON
Executive Commissioner

SPECIAL

VICTORIAN COMMISSION FOR GAMBLING REGULATION

KENO TECHNICAL STANDARD

Version 1.1

November 2011

Table of Contents

1 GLOSSARY

This chapter sets out the glossary of standard terms and abbreviations used by the VCGR and relevant to the Keno Technical Standard

Term or Abbreviation	Description
Act	Means the **Gambling Regulation Act 2003** (Vic.) and Regulations, as amended from time to time.
Baseline	A snapshot of an evolving system. The baseline also defines an envelope around a system (defined by the VCGR) of which the VCGR maintains verification control over. For example application files within a baseline would need approval prior to being modified, and there must be a method in place to verify baseline files have not changed since the last approval.
Central Keno System	The centrally located Component(s) of the Keno System that controls the Keno System and provides information and services to other Components of the Keno System.
Component	Keno-specific devices listed in Section 3.2.1
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.
Cryptographic Data Security	Refers to the protection of critical communication data from eavesdropping and/or illicit alteration.
Entry/Entries	The process of purchasing a right(s) to participate in a Keno Game.
Firewall	Part of a computer system or network that is designed to block unauthorised access while permitting authorised communications.
Firmware	The layer of fixed programs and data structures between the software and hardware that internally controls the hardware and electronic devices.
Hardware	All physical Components (electrical and mechanical) making up the Keno System.
Help Desk	A service by the Licensee that provides information and assistance to Keno System network users.
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 section 10.5 of the Act to represent the VCGR in undertaking inspections of the Keno System.
I/O Channel	The physical interface that controls the transfer of data between the computer and peripheral devices.

Term or Abbreviation	Description
Jackpot	An arrangement where contributions are made to a special jackpot prize pool from which payments, either as cash or merchandise, are made to players.
Keno Game	Has the same meaning as defined in the Act.
Keno Licence	Means the licence granted and issued under the Act by the Minister to authorise the conduct of Keno Games.
Keno Rules	The rules made by the Licensee in accordance with section 6A.2.11 of the Act.
Keno System	Has the same meaning as defined in the Act.
Keno Terminal	A device used for selling, paying and cancelling Entries and other transactions associated with the game of Keno.
Keno Venue	Has the same meaning as defined in the Act.
LAN	Local Area Network, a computer network covering a small physical area.
Licensee	Means the holder of the Keno Licence.
Memory	An area of a computing device used to store data and/or instructions.
Prorating	Circumstances where prizes in a Keno Game are reduced, due to an excess of winners during that game, in accordance with the Keno Rules.
RAM	Random Access Memory – the storage facility used by the CPU to store data and instructions. This form of storage is volatile: if the device in which it is installed loses power, the contents of RAM are lost.
Related Agreement(s)	Means an agreement or agreements dealing with matters related to the Keno Licence referred to in section 6A.3.10 of the Act.
Revision Level	A term used in Configuration Management and Version Control. A Revision Level defines a baseline configuration of a system. Changes may be identified by a number or letter code, termed the 'revision number', 'Revision Level', or simply 'revision'.
RNG	Random Number Generator – a method of producing a sequence of random numbers.
Roll of Manufacturers, Suppliers and Testers	Has the same meaning as defined in the Act.

Term or Abbreviation	Description
Significant Event	In regard to the Keno System: (i) A breach or failure of the physical security; (ii) A breach or failure of the electronic or software systems; (iii) Unauthorised modification or interference; (iv) Unauthorised access or attempted access (whether by electronic or other means); or (v) An event that is prescribed in section 4.5 of the Keno System Requirements Document.
Simulated Racing Game	Computer generated racing game where the outcome of the game is determined by a random number generator drawing a set of numbers from a larger pool of numbers.
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 Section 3.4.61.1 (c) of the Act.
UPS	Uninterruptible Power Supply (a no-break mains power supply including battery backup equipment).
VCGR	Victorian Commission for Gambling Regulation
Version Control	The management of changes to documents, programs, and other information stored as computer files. Also known as revision control, source control or source code management. May be identified by a number or letter code, termed the 'revision number', 'Revision Level', or simply 'revision'.
Victoria	The State of Victoria.
WAN	Wide Area Network, a computer network that covers a broad area.

2 FOREWORD

This chapter introduces the background to the Keno Technical Standard

2.1 Keno System

2.1.1 In April 2008, the government announced a new direction for Victoria's post 2012 gambling industry. The announcement marked the end of a comprehensive regulatory review phase of electronic gaming machines, keno and wagering licence arrangements beyond 2012. Under the arrangements, keno was offered as a single, specific 10 year licence.

2.1.2 The objective of the Keno System Requirements Document, ultimately approved as the Keno Technical Standard, was to provide the post 2012 Keno Licensee with a set of technical standards and guidelines that must be met for the implementation of a Keno System in Victoria.

2.1.3 On 25 March 2011 the Minister for Gaming granted a keno licence to Tabcorp Investments No. 5 Pty Ltd. The licence requires the licensee to commence keno in Victoria on 15 April 2012.

3 INTRODUCTION

This chapter introduces the context and the purpose of the Keno Technical Standard

3.1 General Information

3.1.1 The Keno Technical Standard contains the related technical system requirements for a Keno System operating in Victoria.

3.1.2 This document will be used by the Licensee and a Tester to evaluate the system for compliance with the Keno System requirements, or to evaluate changes to a previously approved system for approval.

3.1.3 This document will be used by the Victorian Commission for Gambling Regulation (VCGR) to evaluate compliance by the Licensee with the Keno Licence and Related Agreement(s), and to evaluate changes to a previously approved Keno System, in accordance with the **Gambling Regulation Act 2003** (the Act). In the event, and to the extent of any inconsistency between the requirements specified in this document and the Act or associated Licence and Related Agreement(s) conditions, the Act and/or associated Licence and Related Agreement(s) conditions will prevail.

3.1.4 All references in this document pertaining to the Licensee refer to the entity licensed to conduct the Keno activity identified by its Licence and Related Agreement(s).

3.1.5 Requirements for the VCGR's revenue audit, compliance verification audit, disaster recovery, and ICT service management are also defined in this document.

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

The Act

3.1.7 The requirements specified in this document are supplementary to and do not take the place of any of the requirements of the Act or associated Licence and Related Agreement(s) conditions (if any).

3.1.8 In approving the Keno System or changes to an approved system, the VCGR may take into account the certificate of a Tester under the section of the Act applicable to the Keno activity.

Objectives

3.1.9 The VCGR sets high systems integrity standards for a Keno System operating in Victoria for the purpose of ensuring that:

i) The system operates in accordance with the Keno Rules for the associated Keno activity;

ii) The system is fair to players;

iii) The system operates in a manner that is auditable, reliable and secure; and

iv) All parties receive their correct entitlement.

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

Document Scope

3.1.11 The requirements in this document apply to the Keno System to be operated by the Licensee according to the Keno Licence and Related Agreement(s) at central locations and Keno Venues in Victoria and at a disaster recovery site in Australia.

3.2 Keno System Design

3.2.1 The VCGR expects that the Keno System will consist of the following Components:

i) A main host computer system, which provides Keno as a rapid draw lottery or Simulated Racing Game;

ii) A device for selecting the required numbers for each game and that provides computer generated random results using an approved Random Number Generator;

iii) Data communication links to each of the venues that are to operate Keno;

iv) Operator driven Keno Terminals used for selling, paying and cancelling Entries and other transactions; and

v) A display system for displaying representation of Keno Games, results of Keno Games and other information relative to the game of Keno.

3.3 ICT Service Management Framework

3.3.1 In order to ensure that the Keno Systems and equipment operate as approved by the VCGR, the Licensee must establish and maintain policies, standards and procedures that the Licensee will use to develop, implement and operate a Keno System, including but not limited to:

i) Service desk, incorporating the Help Desk;

ii) Incident management;

iii) Problem management;

iv) Change management;

v) Release management;

vi) Configuration management;

vii) Application management;

viii) Availability management;

ix) Capacity management;

x) Service level management;

xi) Financial management;

xii) Service continuity management;

xiii) Security management; and

xiv) ICT infrastructure management.

3.3.2 Within the ICT Service Management Framework, the Licensee must establish and maintain Quality Management Systems[1] that meet ISO 9000[2] or an equivalent standard.

3.3.3 Within the ICT Service Management Framework, the Licensee must establish and maintain Information Security Management Systems[3] that meet ISO 27000[4] or an equivalent standard.

3.4 Operational Requirements

Provision of Information

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

3.4.2 When the system is being evaluated for approval, the Licensee must provide sufficient information and documentation to enable a full determination of the system's level of compliance with this requirements document.

---

[1] The organisational structure, procedures, processes and resources needed to implement Quality Management.

[2] A family of standards for Quality Management Systems.

[3] A set of policies concerned with information security management.

[4] A family of standards for Information Security Management systems.

System Performance Standards

3.4.3 The Keno System must be capable of meeting the relevant performance standards set out in the Keno Licence and Related Agreement(s).

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

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

3.4.6 The Keno System must be capable at all times of determining whether all Components of the Keno System that operate software or firmware in connection with Keno Games are functioning.

Responsibilities

3.4.7 The Licensee must adhere to the responsibilities detailed in the Licence and Related Agreement(s).

3.5 Approved Keno System

3.5.1 Only a Keno System approved by the VCGR may be operated in Victoria.

3.5.2 Approval must be obtained from the VCGR for any machinery, equipment or computer system used in connection with Keno Games or that is capable of affecting the integrity and conduct of the game, as determined by the VCGR, before such equipment becomes part of the Keno System.

3.5.3 Each Component of any one hardware revision level shall be identical.

3.5.4 A Component of the Keno System may have multiple suppliers of major assemblies, but approval must be obtained from the VCGR for each Component from each supplier. Off the shelf and custom built Components of the Keno System are required to meet a minimum standard equivalent to the equipment submitted for approval.

4 KENO SYSTEM REQUIREMENTS

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

4.1 Keno System Environment

4.1.1 The VCGR requires that the Licensee implement a computerised Keno System capable of meeting the following broad functions:

i) Efficiently perform all tasks associated with operating a Keno Business;

ii) Comply with the requirements of the Act, Regulations and applicable Licence and Related Agreement(s) conditions (if any);

iii) Comply with the applicable Keno Rules in force at the time;

iv) Comply with the predicted system load requirements;

v) Provide adequate system audit and security requirements;

vi) Provide adequate financial verification and audit capabilities; and

vii) Provide monitoring and reports as required by the VCGR.

4.1.2 The Keno System shall be designed in consideration of the following usability principles:

i) Visibility of system status, keeping users informed through appropriate feedback within reasonable time.

ii) Words, phrases and concepts familiar to the user, rather than system-oriented terms, in a natural and logical order.

iii) Facility to correct a mistake (undo or redo the action) without having to go through an extended dialogue.

iv) Platform conventions that ensure words, situations, or actions mean the same thing.

v) Design which prevents error-prone conditions or checks for them and presents users with a confirmation option before committing an action.

vi) Minimise the user's memory load by making objects, actions, instructions and options visible or easy to retrieve whenever appropriate.

vii) Flexibility and efficiency of use through design that caters to both inexperienced and experienced users and allows users to tailor frequent actions.

viii) Aesthetic and minimalist design that excludes information which is irrelevant or rarely needed.

ix) Help for users to recognise, to diagnose, and to recover from errors including error messages that are expressed in plain language (no codes), and appropriate to their level of training, precisely indicate the problem, and constructively suggest a solution.

x) Help and documentation that is easy to search, is focused on the user's task and lists concrete steps to be carried out.

4.1.3 Publicly accessible Components of the Keno System shall be designed in consideration of the Whole of Victorian Government ICT Standard for Accessibility, available from the eGovernment Resource Centre[5], maintained by the eServices Unit, Information Victoria – a unit within the Department of Innovation, Industry and Regional Development (DIIRD).

Electrostatic Interference

4.1.4 When subjected to human body or any other source of electrostatic discharges, a Keno System Component must not severely interfere with any other connected Keno System Component.

---

[5] http://www.egov.vic.gov.au

4.2 Central Keno System Accommodation

Physical Security

4.2.1 The Central Keno System computer room(s) must be a secure area where only authorised personnel can enter. The VCGR requires the adoption of an electronic locking system that provides monitoring information on the entry and exit of all personnel.

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

4.2.3 There must be a detection system that records an audit log entry, and must provide an alert when unauthorised entry to the computer room is attempted.

Environmental Monitoring System

4.2.4 All machinery, equipment and computer systems within the Central Keno System computer room(s) environment must be supported by an environmental monitoring system.

4.2.5 The environmental monitoring system must be able to check the parameters of the environment that are required for the safe and continual working operation of the Keno System and to automatically alert if these conditions are not met.

Power Supply

4.2.6 All machinery, equipment and computer systems within or contributing to the Central Keno System computer room(s) environment must be supported by at least one Uninterruptible Power Supply (UPS), and at least one stand-by generator.

4.2.7 Policies, standards and procedures must be established and maintained to enable computer systems to be shut down in a controlled and auditable manner without the loss of data, and must include provision should a UPS or stand-by generator fail.

4.2.8 If the supply of mains power to a Central Keno System Component is disrupted, the Component must not severely interfere with the operation of any other Keno System Component, including a Component that is external to the Central Keno System environment.

4.2.9 The UPS, stand-by generator, emergency lighting and any systems or procedures referred to herein, or otherwise essential to the operation of a Keno Business, must be tested at least every three months. These reports will only be required by the VCGR, when the VCGR conducts an audit.

4.2.10 Testing of these procedures and facilities must be logged, and the logbook or equivalent record, as well as other relevant documentation, must be available for inspection by the VCGR, and the VCGR may be in attendance at any test.

Uninterruptible Power Supply (UPS)

4.2.11 The computer, security and telecommunication systems within or contributing to the Central Keno System must be protected against power fluctuations and temporary loss by installation of a UPS or other such device.

4.2.12 The UPS must provide sufficient supply to support the Central Keno System for up to two hours continuous power supply on full load until a stand-by generator is started and enable the systems to be shut down in an orderly manner without the loss of data, should the generators fail.

4.2.13 All machinery, equipment and computer systems situated in the Central Keno System computer room must be earthed via the UPS.

Stand-by Generator

4.2.14 The Central Keno System must be protected against loss of power by the installation and maintenance of a generator or other such device. The generator must have the capacity to support the computer systems, air conditioning, security system, telecommunication equipment, computer terminals, environmental monitoring system and sufficient lighting for normal operation of the Central Keno System and facilities for a period of not less than 24 hours.

Emergency Lighting

4.2.15 The Central Keno System computer room must have an emergency lighting system that automatically lights when mains power is lost. If this operates from the UPS, there must be sufficient capacity in the UPS to cater for the lights, plus computers and air conditioning.

Help Desk System

4.2.16 A 'Help Desk' facility must be provided to assist customers and participating Keno Venues and personnel with problems, disputes and maintenance calls and be available whenever Keno is scheduled through any distribution arrangements or medium, and be available at least one hour before and at least one hour after Keno is scheduled in any Keno Venue.

4.2.17 The Help Desk operators are to have secure on-line access to the Keno System to enable them to perform these activities.

4.2.18 The Help Desk system must enable direct access to multiple Help Desk operators via a call to a dedicated number. There must be sufficient capacity on this dedicated number for customers and participating venues and venue operators to establish contact with Help Desk operators during critical events without unreasonable delay.

4.2.19 All calls to the Help Desk must be logged and the log made available to the VCGR upon request. The information recorded in the log must include, but is not limited to:

i) The time and date the call was made to the Help Desk;

ii) The person making the call;

iii) The issue prompting the call; and

iv) Details of the outcome of the call.

4.3 Central Keno System Host

4.3.1 The Central Keno System must operate in accordance with the Keno Rules as consented to by the VCGR and any regulations associated with operating a Keno Business.

4.3.2 VCGR approval must be obtained for the software configuration (baseline) of the Central Keno System host.

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

System Baseline Document

4.3.4 The Licensee must prepare and maintain a System Baseline Document.

4.3.5 The Licensee must not access or undertake any changes to the system baseline without approval by the VCGR.

4.3.6 The system baseline must include system software and hardware Components, and network and communication infrastructure, that enable the system to operate in a secure environment and meet the legislative and regulatory requirements.

4.3.7 The Licensee, with assistance from a Tester if necessary, must document all system Components, and related configuration items, and identify those that are core to operating a Keno Business (the baseline) to be submitted to the VCGR as part of the request for system approval.

4.3.8 The System Baseline Document must include at least the following:

i) All the system Components which represent the core Components of the Keno System for operating a Keno Business;

ii) Application files, including but not limited to those associated with system or user account access, audit logging, security control, event control, player fairness and revenue reporting;

iii) Operating systems which provide a secure environment;

iv) Interface modules with databases used by the system application;

v) Interface software that interacts with any neighbouring application, external system, remote outlet or third party services;

vi) Central systems communication devices that interface with any neighbouring application, external system, remote outlet or third party services or equipment;

vii) The method and mechanisms 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 Keno System network, including but not limited to 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) The procedure for handling system changes in general;

x) The procedure for handling emergency system changes;

xi) The procedure for maintaining the System Baseline Document, including any emergency changes; and

xii) Any other operation or procedure that is relevant to securing control of the system.

4.3.9 Emergency changes to the Keno System must be notified to the VCGR prior to being applied, including submission of the details of the problem and provided the changes are solely for the purpose of resolving the emergency. The Keno Operator must have appropriate internal procedures in place to provide for internal authorisation for the change. A subsequent Tester recommendation and an application for VCGR final approval are required for all emergency changes as soon as practical after the change has been applied.

4.3.10 A Tester recommendation is required for all changes to the system baseline document, including any emergency changes.

4.3.11 VCGR approval, having regard to any relevant Tester recommendation, must be obtained for any changes to the baseline document, including any emergency changes.

4.3.12 In order to establish a baseline document, an agreement must be reached with the VCGR regarding the directories in which application files will be located on the Central Keno System computers. Files that cannot be verified because they change frequently are not expected to include functionality that would be in the baseline, nor be stored in system application directories.

4.3.13 The Central Keno System must have a method to verify the baseline system application executable files (and selected command utilities) in order to confirm that the configuration of the system is operating in an approved state. The configuration of the system must ensure that any system application executable files (and selected command utilities) residing on storage devices or in the memory of the host Central Keno System are only executable for the Keno System operating in Victoria.

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

Central Keno System Software Procedures

4.3.15 The Licensee must establish and maintain policies, procedures and standards in accordance with the requirement at 3.3 of this document.

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

4.3.17 Only approved application files within the baseline may reside on storage devices or in the memory of the host Central Keno System computers.

4.4 Central Keno System Software Quality

Software Version Control

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

Software Verification During Development

4.4.2 The Licensee and/or its suppliers must establish policies, procedures and standards to ensure the software on which a Tester evaluation was performed is the same as the software submitted to the VCGR for approval and live operation.

4.4.3 The following goals must be met:

i) The Tester must verify and confirm that all the system software being submitted for approval is the same as that which was evaluated;

ii) Only the system baseline files are required to be included with the submission for approval;

iii) A procedure is established which outlines the method for verifying that the executable software on the production system is operating in an approved state; and

iv) A procedure is established which outlines the method for detecting unapproved programs, command files, fixed data files, and any other unauthorised configuration item that reside on any modules in the Keno System.

Central Logging of Information

4.4.4 All security logs must be reviewed and preventative or corrective actions must be undertaken by the Licensee in a timely manner.

4.4.5 All accounting and any security event data must be held and be able to be accessed or retrieved for:

i) Significant events – at least 2 years; and

ii) Financial data – at least 7 years.

Retention of Unclaimed Moneys and Dormant Accounts

4.4.6 The Licensee must securely maintain a register of all dividend money that has not been claimed as required by relevant legislation.

4.4.7 The Licensee must securely maintain a register of all dormant accounts as required by the Licensee's dormant account policy.

4.4.8 The serial numbers or other access method for 'old' unclaimed monies stored on the system (e.g. unclaimed payout / prize tickets), must be secured, and 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.

Financial Summary Reporting

4.4.9 A report which details the financial summary for each Keno Terminal for each Keno Venue, and totals for all terminals is to be provided daily to the VCGR.

4.4.10 The following minimum information is required in a system-wide financial report :

i) Transactions on and current amount of the prize fund;

ii) Sales;

iii) Cancels;

iv) Pays;

v) Voucher sales and redemptions;

vi) Keno Licensee and Keno Licensee Agents cheques;

vii) Jackpot transactions;

viii) Theoretical liability;

ix) Government share of revenue; and

x) Account deposits and withdrawals.

Program Storage Devices

4.4.11 VCGR approval must be obtained for the method of program storage and the method(s) for modifying programs for all devices.

4.4.12 Any Component of the Keno System that maintains its program and/or important statistical data in RAM must be equipped with a backup power supply capable of maintaining for a period of 30 days the information in that RAM.

Keno System Serial Numbers

4.4.13 All serial numbers used in the Keno System must be uniquely identifiable and created by a secure and tamper proof algorithm.

4.5 Significant Events

Generation of Significant Events

4.5.1 The Licensee must establish and maintain policies, procedures and standards for reporting Significant Events to the VCGR in a format to be determined by the VCGR, including but not limited to:

i) Situations where the system is incapable of supporting the Keno Rules;

ii) System failures;

iii) Instances where there has been any form of unauthorised access to any Component of the Keno System;

iv) Instances where non-compliance with policies, procedures or standards is detected, or they were unable to be adhered to;

v) Situations where system hardware, operating systems or any form of system software version roll-backs or reinstallation were carried out;

vi) Instances of the installation and registration of new Keno Terminal equipment;

vii) Instances where significant work-around was carried out by the Licensee;

viii) Instances where a system verification test result produced an unexpected or incorrect outcome;

ix) Instances where late closures were identified, meaning when the stop-sell function does not activate (for any reason) but the RNG does;

x) Instances where incorrect payouts / prizes were identified;

xi) Instances of prorating;

xii) Jackpot wins;

xiii) Payments in excess of designated dollar values;

xiv) Central Site Cheque creation and processing; and

xv) Changes to prize tables, jackpot parameters or prorating parameters.

4.5.2 Where this document states that the Keno System must detect and record Significant Events, it does not imply a particular implementation.

Storage of Significant Events

4.5.3 The Significant Events prescribed by the VCGR, regardless of the source of these events, are to be stored at the Licensee's premises.

4.5.4 All Significant Events must be stored electronically in a manner approved by the VCGR.

4.5.5 A date and time stamp (when the event occurred) must mark each record in the file and it must be possible to retrieve events in a serial fashion.

4.5.6 Significant Events may also be stored in subsidiary points of the Keno System.

Recovery of Significant Events

4.5.7 In the event of the failure of the central system database it must be possible to electronically recover the Significant Events using a method that ensures no Significant Events are lost.

4.6 End of Keno Game Processing

Keno Game Number Increment

4.6.1 When the Keno Game is closed, an end-of-Keno-game record is to be written to a log file and then the current Keno Game number is to be incremented.

4.6.2 Any Entries placed, including those that might have been 'in transit' to the Central Keno System, are to be associated with the new Keno Game number, not the old.

Late Cancels

4.6.3 The Licensee may apply to the VCGR for a scheme to facilitate late cancels.

4.6.4 The Keno System is to prevent Late Cancels once the first number is selected.

Entries During a Draw

4.6.5 The VCGR may approve restricted Entries during the number drawing sequence, defined to be the time from Stop Sell[6] to Confirm Results[7], which includes the number drawing selection and end of Keno Game processing.

4.6.6 Entry restrictions during a draw are as follows:

i) Selling is permissible if the Keno Game number for the Entry is the new Keno Game number(s);

ii) The only cancels permitted are those for tickets sold for future Keno Games after the Keno Game being drawn was closed, i.e. it is not permitted to cancel any Entries sold before the Stop Sell;

iii) Pays are permitted only if the Entry is not active in the Keno Game which is being completed; i.e. all forward games must have been finished before the Keno Game which is currently being drawn or processed. The VCGR may approve pays of small winners (i.e. less than the prorating limit) during the end of Keno Game processing interval if it is satisfied that there are no security problems caused by this; and

iv) Others transactions such as deposits, withdrawals, cash-in, cash-out, login, logout, etc. are permitted in this period.

Keno Results Processing

4.6.7 Once all results are received from the RNG and results have been confirmed, the Keno System must perform the following actions:

i) A Keno results record is to be written to a log file which contains, among other things, the numbers of the balls that have been drawn.

ii) If jackpots are active, the Keno System must scan all active Entries for this game to determine if there are any jackpot winner(s). The prize amounts for each jackpot are to be calculated as per the Keno Rules and the jackpots that have been won must be reset as per the Keno Rules. A Significant Event for the jackpot(s) won must be generated and reported to the VCGR in accordance with 4.5 of this document.

iii) If prorating of winners is specified in the Keno Rules, the Keno System must scan all active Entries for winners that might qualify for prorating (for example, large wins) as per the Keno Rules. If the sum of these prizes exceeds a limit as specified by the Keno Rules, a prorating factor must be calculated and for all of these, large prize amounts are to be adjusted by the prorating factor as per the Keno Rules. A Significant Event for the prorating must be generated and reported to the VCGR in accordance with 4.5 of this document.

[6] Stop Sell means the point of cessation of selling tickets in the current game.

[7] Confirm Results means the point at which results from the current game have been confirmed.

iv) The Keno system must maintain enough information to enable all tickets that are winners in that game to be paid the correct amount when submitted for payout regardless if the ticket is a jackpot win and/or prize table win, prorated or not.

4.7 Central Keno System Security

4.7.1 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 audit ability.

4.7.2 The operating system of the computer's application files and database must provide comprehensive access security.

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

i) Initial password change on its first use must be enforced;

ii) An appropriate minimum password length policy must be enforced;

iii) An appropriate methodology for the enforced frequency of unique password changes and restriction of password re-use;

iv) Procedures for password checking against a list of invalid names (dictionary checking); and

v) Procedures for adequate protection of emergency passwords.

4.7.4 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:

i) Unauthorised attempts to access a system account;

ii) Unauthorised attempts to access a user account;

iii) Unauthorised attempts to access system resources;

iv) Unauthorised attempts to view or change system security definitions or system security rules;

v) Unauthorised attempts to add, modify or delete critical system data;

vi) Irregular patterns of use for system or user accounts;

vii) Irregular or unexpected changes to security configuration; and

viii) Significant authorised changes to security configuration.

4.7.5 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.

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

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

4.7.8 A program must be available that will list all registered users on the system including their access level and a record of no less than 12 months of activity history by the registered user, and this list must be kept current and available at all times for inspection by the VCGR.

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

i) Prize table changes.

ii) Jackpot parameter changes;

iii) Other system parameter changes;

iv) Installation of new versions of software; and

v) Others as determined by the VCGR.

4.7.10 The Licensee must develop and maintain policies and operating procedures designed to prevent hacking or unauthorised access to its Keno System.

4.7.11 The Licensee must ensure that an accredited external and independent Information Technology Network and Security Testing company undertakes system and network vulnerability and penetration testing on its Keno System at least every twelve months and provide a written report of its findings. This report must be provided to the VCGR 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.

System Audit

4.7.12 The Licensee must establish and maintain policies, procedures and standards for system audit matters, including but not limited to:

i) Adequate system security procedures and policies are in place, including security reviews conducted at least every three months;

ii) Critical issues management;

iii) Audit log monitoring, including preventative and corrective actions;

iv) Database security and control, including configurable parameters to protect the integrity of the system;

v) Software integrity;

vi) Peripheral equipment integrity;

vii) User access, including restriction of user access by menu items;

viii) Remote access, including monitoring and preventative or corrective actions for relevant security breaches;

ix) Network and communications security, including prevention, detection and correction measures for relevant security breaches;

x) System interfaces, including management of neighbouring applications, external systems, remote outlets and third party services;

xi) Production environment security, including prevention, detection and correction measures for relevant security breaches;

xii) Software change control aligned with change management processes;

xiii) Emergency change control; and

xiv) The use of data editors, utilities or related software, such as SQL, for database access or update (manual or otherwise) whilst ensuring these are not accessible by unauthorised persons.

4.8 Central Keno System Recovery

Transaction Logging

4.8.1 A complete log of transactions since the last backup is to be maintained at a secure backup site, which must meet the standards required for the primary site as set out in this document.

4.8.2 For transaction logging the Licensee must ensure that:

i) The Central Keno System records (with time/date stamp) all vital transactions received from any equipment that processes a gambling transaction;

ii) The log file(s) and/or database(s) must be duplicated for integrity and reliability;

iii) The method of transaction logging will be assessed prior to approval by the VCGR; and

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

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

4.8.4 There must be no possible means of 'adding records' to the middle of the log or 'writing over' existing records.

4.8.5 There must be no possible means of adding to, amending, 'writing over' or deleting any transaction, record or data contained in the log of existing records.

Format of Log Records

4.8.6 All log records must have a standard format, for which approval must be obtained from the VCGR, and the following minimum information is to be included with each log record:

i) The date that the transaction/event occurred;

ii) The time that the transaction/event occurred;

iii) The identifier for the part of the Keno System for which the transaction/event occurred;

iv) A unique event identifier which defines the transaction/event;

v) The Keno Game number when the transaction/event occurred, where appropriate; and

vi) Any relevant data that is associated with the transaction/event.

4.8.7 A list and description of all transaction/event id's must be provided to the VCGR, and must be kept up to date by the Licensee as modifications are made to the system.

Logging of Keno Entries

4.8.8 The relevant data that must be logged for a Keno Entry is:

i) Starting game number;

ii) Where the Keno Rules allow more than one game to be Entered, the number of games selected;

iii) If a simple Entry, the number of spots and the numbers selected;

iv) Where the Keno Rules allow a combination Entry, the various groups (also known as ways) selected, the range of number of spots selected and the total number of combinations;

v) The unit Entry amount; and

vi) The total Entry amount.

Disaster Recovery and Business Continuity

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

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

4.8.11 The Licensee must establish and maintain policies, procedures and standards for business continuity and disaster recovery.

4.8.12 The Licensee must establish and maintain a business continuity plan, and a disaster recovery plan.

4.8.13 The Licensee must establish and maintain a disaster recovery test plan, including a schedule for testing, for which VCGR approval must be obtained, and conduct disaster recovery testing in accordance with the approved plan.

4.8.14 In the event of a disaster, for example, a fire, there must be a method of ensuring that all data and information related to the Keno System, transactions, player entitlements and government revenue (since the last backup and the transaction log) can be rebuilt up to the point of the disaster.

4.8.15 Copies of all daily database backups must be retained at a secure location other than the primary site, and the secure location must have security policies, procedures and standards equivalent to that required of the primary site.

4.8.16 There must be periodic back-ups (at least daily) of the variable database files on the Central Keno System's storage devices.

System Data Recovery

4.8.17 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 (i.e. the previous night) and fully recover vital transactions via the transaction log up to the point of the failure.

4.8.18 Certain database update information of a non-critical nature may not be required to be automatically recovered. Exceptions of this nature must be identified in the disaster recovery plan, for which approval must be obtained from the VCGR.

4.8.19 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.

Central Site Failure Modes and Recovery

4.8.20 Following any failure, it must be possible to restore the state of the Keno System and its database(s) without losing data as defined in Section 4.8, Keno System Recovery.

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

4.8.22 Some typical tests that may be implemented by the VCGR to test compliance with this and other sections of the Keno System Requirements Document are:

i) Failure of central processor;

ii) Failure of central computer power supply;

iii) Failure of central computer memory;

iv) Failure of central computer disk(s);

v) Failure of central computer I/O channels;

vi) Total power failure of the central site for a short period, (e.g. 30 seconds);

vii) Total power failure of the central site for a long period, (e.g. 30 minutes); and

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

4.9 Data Security

Encryption of Stored Data

4.9.1 The Licensee must encrypt sensitive stored 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)[8].

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

i) PINs; and

ii) Passwords.

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

i) Encryption/Decryption Keys;

[8] http://www.dsd.gov.au/library/infosec/ism.html

ii) If seed information is not logically stored in a password-protected area of the highest access level, then this data must also be encrypted; and

iii) Storage of any complete serial numbers for unclaimed tickets, after the period agreed with the VCGR, and critical fields such as authentication codes.

PIN and Password Management

4.9.4 If a player's or Keno System operator's (or attendant staff) PIN or password is used in support of the system, the PIN or password creation algorithm, its implementation and operational procedures (pertaining to PIN and password changes, database storage, security and distribution) must be evaluated prior to approval by the VCGR.

4.9.5 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.

4.10 Central Keno System Integrity

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

4.10.2 VCGR approval must be obtained for the configuration management plan and the configuration of a Central Keno System.

4.10.3 The Tester will evaluate the configuration for operational integrity as well as recoverability, redundancy and security.

Security of Event Logs

4.10.4 The system must prevent the changing of the Significant Events log and/or significant Keno Entry transactions. 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 (i.e. no random update methods are to be permitted).

Multiple Data Files

4.10.5 Data files and databases that contain vital information must be duplicated for integrity, availability, and reliability.

4.10.6 The Licensee's security policies, procedures and standards, and the mechanisms for ensuring system security, apply equally to production data files and databases and redundant data files and databases.

Documentation and Reporting

4.10.7 Details of the VCGR's reporting requirements will be provided to the Licensee by the VCGR.

VCGR Required Reports

4.10.8 As a minimum, financial information by event conducted must be made available to the VCGR in a format specified by the VCGR that is compatible for processing by the VCGR's systems.

4.10.9 Reports supplied to the VCGR must be complete, comprehensive, accurate, clearly delineated, and available in electronic format.

Central System Integration

4.10.10 The VCGR may approve the integration of sub-systems or utilities with the Keno System, including but not limited to;

i) Performance monitoring systems;

ii) Security systems;

iii) Application management systems;

iv) Environmental monitoring systems; and

v) Any other application that is assisting in the efficient operation of a Keno Business.

4.10.11 The real-time monitoring and inspection facility described in 4.10.15 of this document is not required to be a Component of this approval process.

4.10.12 The integration of the Central Keno System with sub-systems or utilities must be described in the configuration management plan.

Access by the VCGR

4.10.13 The Licensee, at the direction of the VCGR or an Inspector appointed under Section 10.5 of the **Gambling Regulation Act 2003**, must provide access to the information on the Central Keno System application and database at any time.

4.10.14 The Central Keno System software must provide tools and mechanisms to:

i) Examine Significant Events;

ii) Examine data; and

iii) Verify the approved system baseline.

4.10.15 An automated, real-time monitoring and inspection facility must be made available to the VCGR by the Licensee and installed at the VCGR's offices.

4.10.16 This facility must be installed and maintained by the Licensee to ensure consistency with day-to-day operations and applicable Keno Rules.

4.10.17 This facility is not required to be a Component of the system baseline.

Link to VCGR Computing Facilities

4.10.18 The real-time monitoring and inspection facility described in 4.10.15 of this document must include a secure electronic link from the Licensee's Central Keno System site to the VCGR's computer facilities.

4.10.19 The data link between the VCGR and the Keno System must implement Cryptographic Data Security as detailed in Section 5.1 of this document.

4.10.20 The real-time monitoring and inspection facility may be used for down loading financial data and the reports described in 4.10.8 of this document on a daily basis (or at a frequency agreed by the VCGR).

4.10.21 The data link between the VCGR and the Licensee's site must have a data transfer rate to support the real-time monitoring and inspection facility without unreasonable bandwidth-induced delays.

Inspection

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

i) Ability to determine operational hardware and software revision levels;

ii) Ability to view down-loadable software or payout tables, where applicable;

iii) Ability to perform signature checks;

iv) Ability to verify that a Component of the Keno System is on-line;

v) Facilities to support an inspector working together with an inspector in the field;

vi) Other facilities to assist the conduct of inspectors' tasks as necessary for a particular Keno System;

vii) Provision for licensed technicians and special employees to perform all the above;

viii) Ability to review financial meters and (or) data;

ix) Facilities (v) and (vi) to include provision and maintenance of hardware and electronic links at and to the VCGR's premises; and

x) Provision of licensed technicians on request from the VCGR to assist VCGR Inspector's in the conduct of technical compliance.

4.11 Keno Terminal Hardware

4.11.1 VCGR approval must be obtained for the design and configuration of all Keno Terminals and any changes to Keno Terminals.

4.11.2 The Keno Terminal hardware must provide the means for selling, paying and cancelling Entries and other transactions associated with the game of Keno to be carried out in a manner that is auditable, reliable, secure and fair to players.

4.11.3 All banknote acceptance devices used in Keno Terminals must meet the Banknote Acceptance Specifications set out in Section 5 of the Australian/New Zealand Gaming Machine National Standard and Section V6 of the Victorian Appendix to the Australian/New Zealand Gaming Machine National Standard.

4.12 Keno Terminal Functions

4.12.1 VCGR approval must be obtained for all Keno Terminal functions pertinent to Keno Games.

4.12.2 All terminal functions not pertinent to Keno Games must not interfere or affect the outcome of Keno Games or any terminal functions that are pertinent to the Keno Games.

4.12.3 All Keno Terminals and their associated functions must be access protected and must not be capable of any function when an operator is not logged on. All operator functions, including for training, maintenance and technical engineering purposes, must be access protected by a secure access identifier and password or appropriate 'key-lock' facility.

4.12.4 VCGR approval must be obtained for the method and security of communications to and from a Keno Terminal.

5 NETWORK AND COMMUNICATIONS

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

5.1 Cryptographic Data Security

Introduction

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

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

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

Requirement for Cryptographic Data Security

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

i) Cryptographic data security must apply to all critical data that traverses data communications lines. This does not apply to communications within a Keno System computer room.

ii) Cryptographic data security must apply for all critical data communication transfer between all Components of the Keno System at a Keno Venue, and between a Keno Venue and the Central Keno System site (but not necessarily within the Central Keno System site).

iii) Examples of critical data security which would be satisfied by an approved encryption algorithm include:

a) Ticket serial numbers;

b) Encryption keys, where the implementation chosen requires transmission of keys;

c) PINs;

d) Passwords;

e) Customer account information, including but not limited to name, gender, date of birth, address, banking and financial status or transactions;

f) Commercially confidential information, including but not limited to Keno System algorithms and information related to government revenue;

g) Vital transactions related to the operation of a Keno Business; and

h) Email or equivalent communication methods that contain any of the above data or information.

iv) Examples of critical data security which would be satisfied by an approved message authentication algorithm include:

a) Software uploads and downloads of any security related software (e.g. RNG);

b) Transfers of money to/from player accounts; and

c) Transfer of money between Components of the Keno System.

v) There must be a password protected and secure, function to disable encryption to handle circumstances where difficulty with communications is encountered. Disabling of encryption must only occur with the prior approval of the VCGR.

Encryption Algorithm Approval

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

i) Encryption algorithms are to be demonstrably secure against cryptanalytic[9] attacks;

ii) The minimum width (size) for encryption keys is 112 bits;

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

iv) It is not acceptable to only use the current key set to 'encrypt' the next set. An example of an acceptable method of exchanging keys is the use of public key encryption techniques to transfer new key sets.

Message Authentication Algorithm Approval

5.1.6 VCGR approval must be obtained for the message authentication code algorithm, its implementation and operational procedures pertaining. The following are authentication characteristics that will be considered:

i) Message authentication code algorithms are to be demonstrably secure against cryptanalytic attacks;

ii) Message authentication code algorithms are to be designed such that it is feasibly impossible to take a hash value and recreate the original message, 'impossible' in this context means 'cannot be done in any reasonable amount of time.'; and

iii) Message authentication code algorithms are to be designed such that it is feasibly impossible to find two messages that hash to the same hash value.

Encryption Keys

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

5.2 Communications Requirements

Protocol

5.2.1 VCGR approval must be obtained in advance for any protocol used for data communications between Components of the Keno System.

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

5.2.3 The VCGR will only approve a protocol if it is confident that the devices implementing the protocol will fully comply with the requirements of this document.

Data Link

5.2.4 Communications protocols must include the following:

i) Error Control;

ii) Flow Control; and

iii) Link Control (remote connection).

Error Detection

5.2.5 Communications protocols must make use of Cyclic Redundancy Checks (CRC's) or the equivalent – use of only parity or simple checksum byte is not acceptable.

5.2.6 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.

Data Communication Control

5.2.7 Only approved data communication control functions of the Keno System may be implemented. These control functions must be clearly specified in the Baseline documentation.

[9] Cryptanalytic attack is the methods for obtaining the meaning of encrypted information, without access to the encryption key, in an unauthorised way.

Communication Failure Modes and Recovery

5.2.8 All Components of the Keno System must be able to 'gracefully' handle a range of simple failures.

5.2.9 The Keno System must be recoverable to the point of failure following an interruption.

5.2.10 Some typical tests which may be implemented by the VCGR or its representatives to test compliance with this document are:

i) Failure of Central Keno System LAN interfaces;

ii) Failure of central LAN;

iii) Failure of central data communication interface devices;

iv) Failure of a single data communication interface;

v) High data communications error rates on line;

vi) A foreign or additional device placed on a LAN;

vii) A foreign or additional device placed between LAN bridges, communications controllers or on data communication lines between sites;

viii) Single data communication port failure on a remote controller (if any); and

ix) LAN failure on a regional or local controller (if any).

5.3 Network Requirements

5.3.1 This section describes the VCGR's network requirements on system firewalls, network connections that are inside a baseline envelope, and network connections from the baseline envelope to external devices.

5.3.2 A baseline envelope is the core area defined by the VCGR as to be under baseline control, and must be described by the Keno Licensee in a configuration management plan.

Network Baseline

5.3.3 During the approval stage of a system network, the VCGR will confirm the core areas of the system network over which verification control must be maintained and this must be defined and approved in a Network Policy Document.

5.3.4 The Network Policy Document must be established and maintained by the Keno Licensee and must include a matrix that describes the network topology of the system, details of the interconnection of modules within the network and the type of connection between the modules that is permitted.

5.3.5 The Network Policy Document must be reviewed and evaluated by a Tester.

Physical Requirements

5.3.6 Power to devices inside and on the boundary of the baseline envelope must be provided from a filtered, dedicated power circuit. It is intended that devices which can affect or cause damage to Components of the Keno System must be protected by a filtered, dedicated power circuit.

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

Network Documentation

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

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

Connection of External Devices to Networks Inside a Baseline Envelope

5.3.10 Unused ports on network devices and network control devices inside and on the boundary of the baseline envelope must be disabled.

5.3.11 The facilities for plug and play[10] installation of unregulated devices must be disabled.

5.3.12 Host computer systems, network devices and network control devices inside and on the boundary of the baseline envelope must be protected from high loads, including but not limited to broadcast storms, denial-of-service attacks, or faults on any part of the network outside the baseline envelope. Such attacks must not affect system integrity, or the ability to recover from those attacks.

5.3.13 Configuration changes to all devices inside and on the boundary of the baseline envelope must be protected by encrypted passwords. Password protection policies, procedures and standards must exist and be implemented by the Keno Licensee, including provision of prevention, detection and correction measures for non-compliance.

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

5.3.15 At a Central Keno System site, all network devices, network control devices and hosts associated with a production network must be located inside an area that only authorised persons can enter.

Communications Within a Baseline Envelope

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

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

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

5.3.19 All information traversing the network between remote equipment and the Central Keno System host must be recoverable once communications are restored.

Communications between Separate Baseline Envelopes

5.3.20 Information flowing between different baseline envelopes must be subject to authentication and encryption (see 5.1), unless the VCGR has approved an exception that the intervening network is physically and adequately secure and under the complete control of the Licensee.

5.3.21 WAN communication links are deemed to be outside a baseline envelope and VCGR approval must be obtained for any exceptions.

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

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

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

---

[10] A technique by which new hardware may be added to an existing computer and be automatically detected and configured.

5.3.25 Communication between devices in separate baseline envelopes must be protected must be immune from computer/network attacks, including but not limited to hacking, cracking, virus, spy ware, spam or denial-of-service attacks.

Communications to Devices Outside a Baseline Envelope (Firewall)

5.3.26 Data exchanged with computer systems and terminals outside the baseline envelope must pass through at least one network control device (router or firewall).

5.3.27 Network control devices must implement the controls as defined in the Network Policy Document, which must be prepared by the Licensee and submitted to the VCGR for approval.

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

5.3.29 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.

5.3.30 Any person authorised to make configuration changes must not be able to change the audit trail, and an alert must be produced for all unauthorised attempts to change an audit log.

5.3.31 Network control devices must be configured to discard all traffic other than that which is specifically permitted by the Network Policy Document. Configurations that discard specific traffic types and allow everything else are not acceptable.

5.3.32 Computer systems within the baseline envelope must not be affected by computer/network attacks emanating from outside the baseline envelope (e.g. ping-of-death attacks, teardrop attacks, routing protocol attacks, etc.). Such attacks must not affect system integrity, or the ability to recover from those attacks.

5.3.33 Operational procedures for network control devices must include the capturing and regular review and follow-up, including corrective action in a timely manner, of all access violations.

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

i) The message authentication scheme utilised;

ii) The Encryption scheme utilised; Encryption must occur at the boundary and inside the baseline envelope;

iii) Physical security of the network (including intervening hubs, bridges and routers);

iv) Connections to the external devices;

v) The sensitivity of the information being transferred;

vi) Whether the computer system inside the baseline envelope or outside the baseline envelope initiates information transfer;

vii) Audit information recorded on the Central Keno System pertaining to the transfer of files and information; and

viii) Intrusion detection utilised and immunity from computer attacks.

5.3.35 WAN and Internet communication links are deemed to be outside the baseline envelope approved by the VCGR, and VCGR approval must be obtained for any exceptions.

Monitoring Systems and Network Management Systems

5.3.36 VCGR approval must be obtained for any applications or utilities that enable monitoring of Components of the Keno System inside or on the boundary of a baseline envelope for the purposes of availability, configuration or performance management. The process for approval, including any third-party products, is on a ‘case-by-case’ basis.

5.3.37 VCGR approval must be obtained for network monitoring systems that monitor network devices and network control devices inside or on the boundary of a baseline envelope. The process for approval, including any third-party products, is on a 'case-by-case' basis.

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

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

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

ii) Imitating the hardware address (e.g. Ethernet address) of a host monitoring system or a network management system; or

iii) Replaying previously captured communications.

5.3.40 A device outside a baseline envelope must not be able to affect the operation of a central monitoring host and must not be able to read or modify critical data by:

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

ii) Imitating the hardware address (e.g. Ethernet address) of a host monitoring system or a network management system; or

iii) Replaying previously captured communications.

Internet Connections

5.3.41 Internet connections must demonstrate adequate networked 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.

5.3.42 The Keno System, at the point where it is connected to the Internet service provider, must incorporate a DMZ[11] like architecture.

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

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

Verification Tools

5.3.45 The VCGR 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.

5.4 Wireless Communication

5.4.1 Wireless communication may be acceptable to the VCGR 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)[12], to overcome the general weaknesses of wireless communication,

5.4.2 Wireless communication will be considered for Local Area Network communications within venues and/or Wide Area Network communication between venues and the Central Keno System.

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

---

[11] Demilitarized Zone, also known as a Data Management Zone or Demarcation Zone; an additional layer of security to a LAN that provides a physical or logical sub-network to contain system components that enable external services to an un-trusted network, usually the Internet, and prevent intrusion to specific hosts in the internal network.

[12] http://www.dsd.gov.au/library/infosec/ism.html

5.4.4 The access point must not be placed directly onto the venue network unless an acceptable firewall implementation is employed. A firewall that is incorporated into another device, such as a router, may be acceptable. The process for approval, including any third-party products, is on a 'case-by-case' basis.

5.4.5 Wireless network traffic must be secured with additional encryption and/or authentication codes and must meet the requirements of Section 5.1.

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

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

6 TESTING REQUIREMENTS

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

6.1 Inspection and Testing

6.1.1 The VCGR may have regard to a recommendation for system approval from a Tester listed on the Roll of Manufacturers, Suppliers and Testers as defined in the Act.

6.1.2 The Licensee must establish and maintain policies, procedures and standards for quality assurance[13] and control equivalent to ISO9000, and a test strategy that includes consideration of the need to test:

i) Network hardware and communications infrastructure;

ii) System functionality;

iii) System interfaces;

iv) System Usability, in consideration of the requirement at 4.1.2, including ease of use for customer facing devices and graphic user interfaces (GUI);

v) Accessibility in consideration of the requirement at 4.1.3;

vi) User acceptance;

vii) Performance, including consideration of load generation for response, stress, volume and soak testing of system, database and network configurations;

viii) Security, including consideration of testing system and network configurations for vulnerability, penetration, hacking, cracking, virus, spy ware, spam or denial-of-service attacks;

ix) Disaster recovery;

x) Business processes; and

xi) Business readiness, including provision for a live trial when required by the VCGR.

6.1.3 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.

Tester Evaluation

6.1.4 A Tester will work with the Licensee to undertake an evaluation of the Keno System covering aspects including but not limited to:

i) Compliance with the relevant Keno Rules;

ii) Fairness and integrity of new or amended corresponding Keno Rules;

iii) Matrix of Keno products to selling channels;

iv) Accuracy and consistency in the display of information;

v) Functional integrity of communication protocols in use;

vi) Regulatory reporting;

vii) Licensee and/or player access to the Keno System;

viii) Integrity of player accounts; and

ix) Integration or deployment of new technologies.

Facilities for a Tester

6.1.5 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 VCGR accordingly.

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

Test Environment

6.1.6 The Licensee must ensure that upgrades to machinery, equipment and computer systems making up the Keno System can be adequately tested in an appropriate test environment using a test system that is functionally, but not necessarily physically, identical to that proposed for use in production.

6.1.7 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 VCGR.

6.1.8 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.

Failure Modes and Recovery Testing

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

i) Failure of the Central Keno System power supply;

ii) Total power failure of the Central Keno System site:

iii) For a short period (e.g. 30 seconds); or

iv) For a long period (e.g. 30 minutes)

v) Verifying there is no single point of failure;

vi) Individual server capability to sustain persistent load;

vii) Guaranteed messaging;

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

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

x) Failure of Central Keno System I/O channels;

xi) Failure of links with remote interface points; and

xii) Keno System operator error, including but not limited to invalid data entry.

6.2 System Testing Requirements

Testing Requirements and Tester Recommendation

6.2.1 The security and controls, functional specifications, and all the requirements of the system are to be evaluated and recommended by a Tester listed on the Roll of Manufacturers, Suppliers and Testers as defined in the Act.

6.2.2 A Tester recommendation is required on:

i) The system integrity and reliability;

ii) Whether the system meets all the legislative, technical, and reporting requirements;

iii) Whether the controls and procedures required exist and are effective; and

iv) The System Baseline Document and the Network Policy Document for future approval.

Associated Systems Requirements

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

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

Submissions Requirements

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

i) Background of the Keno System;

ii) Purpose of the submission;

iii) Description of the scope of system and operational changes;

iv) List / description of all machinery, equipment and computer systems within the Keno System;

v) Description of all networks within the Keno System;

vi) Tester recommendation regarding the Keno System in accordance with above requirements;

vii) The Licensee's comments on any conditions included in the Tester's recommendation;

viii) List of all software versions and associated CRCs;

ix) List of all relevant hardware and operating systems – product names, models and versions;

x) Associated systems that are connected to the Keno System;

xi) A Keno System Baseline document; and

xii) A Network Policy Document (if applicable).

Environmental Testing

6.2.6 Suppliers of machinery, equipment or computer systems used in connection with Keno Games are to provide information as to the range of environmental extremes at which the machinery, equipment or computer system(s) will continue to operate normally and must have conducted environmental testing to demonstrate the equipment's specified maximum and minimum extremes of temperature and humidity.

6.2.7 The VCGR requires the equipment to run within the equipment's own environmental specifications.

7 PLAYER ACCOUNT REQUIREMENTS

This chapter sets out the Keno System requirements for player accounts that must be met for all Keno activities carried out in Victoria.

7.1 Player Accounts

7.1.1 Account based Keno activities must only be available to players who are pre-registered and hold a player account with the Licensee.

7.1.2 The Keno System must not accept an Entry that would cause a player account to become negative.

7.2 Creation of Player Accounts

7.2.1 Only natural persons over the age of 18 years are permitted to create a player account.

7.2.2 If any person has more than one active player account, they must be linked to a master account or record.

7.2.3 The Licensee must have carried out a Proof of Identity check on each applicant before an account can be created in the Keno System.

7.2.4 The Licensee must securely maintain a register of player verifications.

7.2.5 Upon registration in the Keno System, each player must be allocated a unique identifier to enable identification of the appropriate player and account details by the Keno System each time a player commences a session.

7.2.6 The Licensee must securely maintain a register of player accounts.

7.2.7 The Keno System must facilitate the deactivation of a player's account and re-registration.

7.2.8 A new account for a person must not be created if the deactivation reason for a previous account indicates that the person must not be permitted to establish another account.

7.2.9 The Keno System must meet the requirements of the Licensee's Code of Conduct.

7.3 Privacy of Player Information

7.3.1 Any information obtained by the Licensee in respect of player pre-registration or account establishment must be kept confidential by the Licensee except where the release of that information is required by law or approved by the player.

7.3.2 Any information about the current state of player accounts must be kept confidential by the Licensee except where the release of that information is required by law.

7.3.3 Use of player information in development, testing and production environments must not breach the 'Information Privacy Principles' under section 14 of the Australian Federal Privacy Act and the 'OECD Guidelines on the Protection of Privacy and Transborder Data Flow of Personal Data'.

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

7.3.5 The Licensee must not prevent a player participating in Keno Games for the sole reason that the player refuses to allow the use of personal information for non-Keno Game purposes.

7.4 Player Accounts Maintenance

7.4.1 Storage of money and monetary values on the Keno System must be secured against invalid access or update other than by approved methods.

7.4.2 All deposit, withdrawal or adjustment transactions are to be maintained in a system audit log.

7.4.3 A deposit made using a credit card transaction must not be available for the purpose of placing a Keno Entry until such time as the funds are received from the credit provider or the credit provider issues an authorisation number to the operator indicating that the funds are guaranteed. The authorisation number is to be maintained in a system audit log.

7.4.4 Positive identification, including PIN entry, must be made before withdrawal of monies held by the Keno System can be made.

7.4.5 Inactive accounts holding monies held in the system must be protected against forms of illicit access or removal.

7.4.6 All transactions involving monies are to be treated as vital information to be recovered by the Keno System in the event of a failure.

7.4.7 Personal information of a sensitive nature must only be stored in an encrypted form on the Keno System. 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)[14].

7.4.8 In relation to 7.4.7, personal information of a sensitive nature includes, but is not limited to:

i) Financial Institution account numbers;

ii) Credit and debit card numbers, or equivalent;

iii) Credit and debit card expiry dates;

iv) Card Security Value (CSV) numbers;

v) Expected answers to any questions used to verify a player's identity (e.g. Mother's maiden name); and

vi) Balances of player accounts on the Keno System.

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

i) Financial Institution PINs; and

ii) PINs used by players to access financial details of Keno System player accounts.

7.5 Player Account Statements

7.5.1 An account statement must be available to the player upon request.

7.5.2 Account statements must include sufficient information to allow the player to reconcile the statement against their own records to the session level.

7.5.3 Account statements must also include details of major wins.

7.6 De-activated Player Accounts

7.6.1 Any funds left in an account which is to be de-activated are to be remitted to the owner of the account.

7.6.2 The Licensee must establish policies, standards and procedures relating to how such players will be found in the event they are no longer at their registered address or, in the event of a deceased player, how the rightful recipient is found.

7.6.3 The Licensee must establish policies, standards and procedures regarding the treatment of retention of unclaimed monies and dormant accounts, and the Keno System requirements at sections 4.4.6 – 4.4.7 of this document.

7.7 Player Loyalty

7.7.1 The requirements of this section only apply if player loyalty is supported by the Keno System and promotions involve the use of player loyalty to affect the taxation basis of the Licence, e.g. conversion of player loyalty points into Entries.

7.7.2 The player loyalty database must be maintained separate to any other database(s) and on a secure part of the system.

[14] http://www.dsd.gov.au/library/infosec/ism.html

7.7.3 Use of player tracking data in development, testing and production environments must not breach the 'Information Privacy Principles' under section 14 of the Australian Federal Privacy Act and the 'OECD Guidelines on the Protection of Privacy and Transborder Data Flow of Personal Data'.

7.7.4 Redemption of player loyalty points earned must be a secure transaction that automatically debits the points balance for the value of the prize redeemed.

7.7.5 All player loyalty database transactions are to be recorded as critical data by the Keno System.

7.7.6 A statement of player loyalty transactions must be available to the customer on request.

8 Customer Interface

This chapter sets out the requirements relating to the customer interface that must be met for all Keno System activities carried out in Victoria.

8.1 Available Information

8.1.1 This section refers to requirements for information that is to be made available to Keno System customers.

Keno Game Information

8.1.2 At a minimum, the following information must be available to customers concerning Keno Games:

i) Current game number;

ii) Time until next game;

iii) Current jackpot amounts, if any;

iv) Results of the previous game, if not during a game draw; and

v) Results drawn so far, if during a game draw.

Entry Information

8.1.3 At a minimum, the following information must be available to customers concerning any Entries placed, in words and numbers or words or numbers, as the case may be:

i) The game number(s) for which the ticket is active.

ii) Selections and/or combinations chosen;

iii) An indication of which prize table was selected, if there are more than one available to the players;

iv) Unit Entry; and

v) Total Entry.

8.2 Keno Terminal Entries

8.2.1 This section refers to requirements relating to the use of Keno Terminals to provide Entry facilities to Keno customers.

Keno Displays

8.2.2 Keno Venues will require Keno displays which must indicate at least the game information described in section 8.1.2.

Operator Entered Cash Entries

8.2.3 Operators at Keno Terminals may accept transactions, Entries, cancels and pays as a cash exchange.

8.2.4 Whenever an Entry is placed, a unique ticket must be printed containing the information in section 8.1.3 and a unique serial number to identify the Entry.

8.2.5 A means of including an identifier on the ticket for a terminal to automatically read the serial number, e.g. a barcode, may be acceptable provided it directly reflects the serial number and is not 'easily predicted' from other valid serial numbers.

8.2.6 A means of cancelling cash Entries must be provided – refer to section 8.4.

8.2.7 A means of paying winning or refunded cash Entries must be provided – refer to section 8.5.

8.2.8 Transactions at a Keno Terminal involving Keno System player accounts may be acceptable provided:

i) There is a unique player account identifier entered at the terminal; and

ii) Withdrawal transactions or Entries placed against a player account involve the entry of an account PIN or the equivalent.

Keno System Serial Numbers

8.2.9 All serial numbers used in the Keno System must be uniquely identifiable and created by a secure and tamper proof algorithm.

Self Service Terminals (SST)

Account Based SST Entries

8.2.10 When Entries are made against an existing player account, it is not necessary to print a cash ticket receipt for any Entry but the Entry information of section 8.1.3 and the account balance after the transaction must be made immediately available.

Cash Exchange SST Entries

8.2.11 Alternatively, 'cash exchange' Entries may be made by first inserting money into the SST via banknote, coin or debit card.

8.2.12 A cash ticket receipt must be printed for each 'cash exchange' Entry accepted by the system. In addition, all of the requirements of sections 8.2.4 – 8.2.8 must be met.

8.3 Online Participation

8.3.1 This section refers to requirements relating to Keno System customers placing Entries via terminals connected to communication channels such as the Internet or digital television.

8.3.2 All communications must meet the Cryptographic Data Security requirements of section 5.1.

8.3.3 Before Entry transactions can take place, the customer must log-in to an existing player account with account ID and appropriate security control, e.g. password or PIN.

8.3.4 As Entries are made the Entry information of section 8.1.3 and the account balance after the transaction must be displayed to the customer on the input device, e.g. screen.

8.3.5 A means of cancelling account Entries must be provided – refer to section 8.4.

8.3.6 It must be possible for the player to access the game information of section 8.1.2 and responses must be displayed on the input device.

8.4 Cancelling Entries

8.4.1 The Licensee must obtain VCGR approval of any method for a Keno System operator to cancel a player's active Entry/Entries.

8.4.2 In the event that the Keno System allows an Entry to be cancelled:

i) For a cash Entry that is cancelled, the customer must be refunded any amount the customer paid for the original Entry; and

ii) For an account based Entry, the player's account balance must be immediately updated with the amount of the Entry that was cancelled.

8.4.3 The Keno System may provide a cancellation period-of-grace to allow players sufficient time to cancel Entries placed incorrectly.

8.4.4 Subject to the restrictions of section 4.6.6 and the Keno Rules, Entries with outstanding forward games may be cancelled. If that is the case, the Entry amount for those forward games, the number of games multiplied by the unit Entry amount, plus the sum of any prizes or jackpots won in decided games, if any, is to be refunded / paid to the player. Only Entry amounts paid for outstanding forward games will be refunded.

8.5 Winning Payments

8.5.1 Once the games for each Entry are entirely decided, the Keno System must, for those complete Entries with winnings:

i) If the winning Entry was a cash Entry, make it available for payment at a cash terminal; or

ii) If the winning Entry was an account based Entry, credit the winning amount directly to the player's account immediately or upon the next access to the account.

9 Random Number Generator

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

9.1 Random Number Generator (RNG)

9.1.1 The VCGR requires the use of an appropriate random number generator (RNG) for the selection of the results of electronic Keno products, including Simulated Racing Games.

9.1.2 VCGR approval must be obtained for the RNG algorithm and its use.

Physically Separate RNG unit

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

9.1.4 VCGR approval must be obtained for the physical security of the RNG.

9.1.5 The cage, case or cabinet must be electro-magnetically shielded and physically secure.

9.1.6 The RNG must comply with specific requirements for Electromagnetic interference as detailed in section 2.3 of the Australian/New Zealand Gaming Machine National Standard.

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

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

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

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

Logically Separate RNG

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

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

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

9.1.14 Approval for the logical security of the RNG must be obtained from the VCGR.

RNG Software Storage

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

9.1.16 Prior approval must be obtained from the VCGR each time the RNG program is to be changed.

Duplicated RNG Units

9.1.17 The RNG units must be duplicated – i.e. there must be at least two RNG's available during normal operation:

i) If the RNG is implemented as a physically separate RNG unit, there must be two such units; or

ii) If the RNG software is contained within the Keno System computer systems there must be logically separated software in (at least) the back-up computer system(s).

9.1.18 The VCGR does not require random selection of a RNG device.

9.1.19 A back-up RNG may be an approved 'cold-standby' unit which is swapped in should there be a failure of the primary unit.

Record of Keno Selections

9.1.20 When the RNG has selected the required numbers that are the 'result' of the game, 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.

9.1.21 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.

9.1.22 The recorded output should show at least:

i) Date;

ii) Time;

iii) The Keno Game number;

iv) The numbers drawn;

v) A unique checksum (that is to be entered with the numbers and checked by the Keno System when manual entry of numbers is required); and

vi) Other security information if available.

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

9.2 Communication with a Central System

Method of Communication

9.2.1 VCGR approval must be obtained for the methods of communication from the RNG to the Central Keno System. If serial communication is to be used, refer to Section 5 of this document.

Results in a Single Message

9.2.2 The method of transferring data between the RNG and the Central Keno System computer is to be secure and tamper proof.

Security of Connection of RNG Device

9.2.3 The Keno System and the RNG devices are to be designed to reduce the chance of 'rogue devices' communicating false results to the Keno System host.

9.2.4 Each RNG is to have a uniquely associated code which is sent to and verified by the Keno System whenever the RNG establishes communication with the Keno System.

9.3 Mathematical Requirements of the RNG

9.3.1 Where a Keno product result is determined by a Random Number Generator, the RNG is a vital Component and VCGR approval must be obtained for its implementation and use. Approvals will be based on a number of criteria including the minimum specifications described in this document.

9.3.2 For RNG requirements, refer to section 3.14 of the Australian/New Zealand Gaming Machine National Standard.

9.4 RNG Test Modes

9.4.1 Test versions of the software should provide for production by the RNG of known defined sequences of numbers. Such a list of numbers must be able to be loaded into the machine by the testing officer.

9.4.2 Such a test facility must not exist in the operational software.

9.5 Software RNG versus Hardware RNG

9.5.1 The VCGR recognises that a choice may be available between a software based implementation of a mathematical pseudo random number algorithm and a hardware device that purports to actually generate random quantities.

9.5.2 While the VCGR has no disagreement in principle with either choice, it is considered that it may be more difficult to demonstrate adherence to the various requirements above with a hardware device than with software where the algorithm can be exactly defined and hence its behaviour extensively analysed.

9.6 Chance Keno Game Behaviour

9.6.1 The following rules apply to the use of random number generators relative to chance Keno Game behaviour.

Chance Keno Game Behaviour to be Uncorrelated

9.6.2 Events of chance within games must be independent of (i.e. uncorrelated with) any other events within the Keno Game or any events within previous games.

Chance Keno Game Behaviour not to be Influenced

9.6.3 Events of chance within games must not be influenced, affected, controlled or determined by anything other than (in conjunction with the prevailing payout table) numerical values obtained in an approved manner from the approved RNG.

Adaptive Behaviour

9.6.4 Events of chance within games must not be automatically influenced in any way by recent history or other statistics of player, Keno Game or Keno Venue performance.

Random Number Selection Sequence

9.6.5 The numerical values from the RNG used to determine chance Keno Game events must be obtained in the normal manner and the normal sequence applicable to the type of RNG. The selection, discarding or sequence of usage of such numerical values must not be influenced in any non-approved way.

9.6.6 The action of background RNG generation is considered to be part of the normal operation of a RNG incorporating such a feature, and so the requirement here does not preclude the existence of such a background RNG activity feature.

Chance Keno Game Behaviour to be Frozen

9.6.7 Prior to the commencement of each draw for a Keno Game, all random behaviour to be used during a Keno Game is to be fully determined and frozen.

9.6.8 This requires that all random numbers (including random decisions, random events or any other random behaviour) to be used during the course of the draw for a Keno Game are generated and recorded prior to the start of the draw for a Keno Game.

No Subsequent Decisions

9.6.9 Subsequent to the commencement of the draw for a Keno Game, no subsequent actions or decisions may be made that would change the behaviour of any of the events of chance within the Keno Game play other than player decision.

Chance Keno Game Behaviour to be Recorded

9.6.10 Prior to the commencement of each Keno Game, sufficient information is to be recorded so as to allow all random behaviour to be used during the Keno Game to be able to be fully reconstructed in the event of a Keno Game replay for whatever reason, including all cases of Keno Game recovery following Keno Game interruption.

9.6.11 This requires that all pre-determined information be recorded. The manner of recording must be as for any other Keno Game replay information, that is, in an appropriately non-volatile and/or backed-up medium that will facilitate Keno Game replay and Keno Game recovery.

9.7 Other Uses of RNG Prohibited

9.7.1 The ‘draw’ RNG must not be used for any purpose other than the ‘official’ use as identified by the rules of the Keno product.

9.8 Verification of the RNG Device

Source Software to be Provided

9.8.1 The source software for the RNG device is to be provided to the VCGR and / or Tester in an approved machine readable form. Program and functional documentation should also be provided.

Separate Compilation Required

9.8.2 The VCGR requires the ability to separately compile the RNG program(s) to verify that the programs running are identical to the programs evaluated.

Maintenance of Statistics

9.8.3 Keno product types that require the use of an RNG must maintain a record for each game played and calculate 'reasonableness' statistics on the results of the games in an attempt to identify and warn the Keno System operator of possible non-random performance.

10 DOCUMENT INFORMATION

10.1 Document Details

Criteria	Details
Document title:	Keno Technical Standard
Document owner:	Director, Gambling Operations and Audit, VCGR
Document author:	Gambling Licences Transition Project, VCGR

10.2 Version Control

Version	Date	Description	Author
V1.0	28 June 2011	Keno Technical Standard	VCGR
V1.1	November 2011	Keno Technical Standard	VCGR

10.3 Reference Material

Acronyms	Description
ROI	Registration of Interest
VCGR	Victorian Commission for Gambling Regulation
GLP	Gambling Licences Project

10.4 Approvals

Name	Position	Function
VCGR	The Commission	Make or amend with Ministerial approval

11 RELATED DOCUMENTS

Document Title	Version
Australian/New Zealand Gaming Machine National Standard	V10.0
Victorian Appendix to the Australian/New Zealand Gaming Machine National Standard	V10.0
Keno Licence	25 March 2011
Keno Agreement	25 March 2011

End of Document

This page was left blank intentionally

This page was left blank intentionally

This page was left blank intentionally

bluestar PRINT

The *Victoria Government Gazette* is published by Blue Star Print with the authority of the Government Printer for the State of Victoria

Address all enquiries to the Government Printer for the State of Victoria
Level 2, 1 Macarthur Street
Melbourne 3002
Victoria Australia

How To Order

	Mail Order	**Victoria Government Gazette** Level 5, 460 Bourke Street Melbourne 3000 PO Box 1957 Melbourne 3001 DX 106 Melbourne
✆	**Telephone**	(03) 8523 4601
FAX	**Fax**	(03) 9600 0478
	email	gazette@bluestargroup.com.au
	Retail & Mail Sales	**Victoria Government Gazette** Level 5, 460 Bourke Street Melbourne 3000 PO Box 1957 Melbourne 3001
✆	**Telephone**	(03) 8523 4601
FAX	**Fax**	(03) 9600 0478
	Retail Sales	**Victorian Government Bookshop** Level 20, 80 Collins Street Melbourne 3000
✆	**Telephone**	1300 366 356
FAX	**Fax**	(03) 9603 9920

Price Code D