

Keno Technical Standard

OFFICIAL

2 June 2022

TRIM ID: CD/22/8902

Version: 3.3

Contents

1	Glossary	3
2	Foreword	7
2.1	Keno Technical Standard Evolution	7
3	Introduction	8
3.1	General Information	8
3.2	Keno System Design	9
3.3	ICT Service Management Framework	9
3.4	Operational Requirements	10
3.5	Approved Keno System	11
4	Keno System Requirements	12
4.1	Keno System Requirements	12
4.2	Licensee-operated Central Keno System Environment	13
4.3	Cloud-based computing environment for a Keno System	14
4.4	Help Desk facility	15
4.5	A Keno System	15
4.6	Keno System Software Quality	18
4.7	Significant Events	20
4.8	End of Keno Game Processing	21
4.9	Keno System Security	22
4.10	Keno System Recovery	24
4.11	Data Security	26
4.12	Keno System Integrity	27
4.13	Keno Terminal Hardware	29
4.14	Keno Terminal Functions	30
4.15	Customer application software for online Keno Distribution	30
5	Network and Communications	32
5.1	Cryptographic Data Security	32
5.2	Communications Requirements	33
5.3	Network Requirements	34
5.4	Wireless Communication	37
6	Testing Requirements	39
6.1	Inspection and Testing	39
6.2	System Testing Requirements	41
7	Player Accounts	43
7.1	Player Account capability	43
7.2	Creation of Player Accounts	43

7.3	Privacy of Player Information	43
7.4	Player Accounts Maintenance	44
7.5	Player Account Statements	44
7.6	De-activated and Dormant Player Accounts	44
7.7	Player Loyalty	45
8	Customer Interface	46
8.1	Available information	46
8.2	Keno Terminal Entries at Keno Venues	46
8.3	Online Participation by Player Account holders	47
8.4	Cancelling Entries	48
8.5	Winning Payments	48
9	Random Number Generator	49
9.1	Random Number Generator (RNG)	49
9.2	Communication with a Central System	51
9.3	Requirements of the RNG	51
9.4	RNG Test Modes	51
9.5	Software RNG versus Hardware RNG	51
9.6	Chance Keno Game Behaviour	52
9.7	Other Uses of RNG Prohibited	53
9.8	Verification of the RNG Device	53

1 Glossary

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

Term or abbreviation	Description
Act	Means the <i>Gambling Regulation Act 2003</i> , as amended from time to time.
Baseline	The term baseline refers to all components that are defined as core to the Keno System by the Licensee and approved by the Commission at a point in time, that thereafter serves as the basis for defining incremental changes to the Central Keno System.
Baseline Envelope	This term refers to an envelope around a Keno System over which the Commission maintains verification control.
Central Keno System	The centrally located Component(s) of a Keno System that controls a Keno System and provides information and services to other Components of a 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.
Critical Data	Information including, but not limited to: <ul style="list-style-type: none"> • game • draw • result information • security events • ticket serial numbers • RNG seeds • signature seeds (algorithm coefficients) • signature results • encryption keys • PINs • passwords • software uploads and downloads of any security related software

	<ul style="list-style-type: none"> • transfer of money between computer equipment • any changeable configuration information • unclaimed tickets
Cryptographic Data Security	Refers to the protection of critical communication data from eavesdropping and/or illicit alteration
Data	Means all data and expressions of data contained in, or processed or generated by, a Keno System including without limitation: <ul style="list-style-type: none"> • all data and expressions of data comprising reports generated by a Keno System • all data and expression of data about or relating to or generated by Agents and contractors stored within a Keno System.
Emergency Changes	Changes to any component of a Keno System that are deemed urgent and immediately necessary to assist in resolving a failure of a Keno System and restoration of normal services.
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 a 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
Inspectors (s)	A person who is appointed under legislation to represent the VGCCC in undertaking inspections of a Keno System.
I/O Channel	The physical interface that controls the transfer of data between the computer and peripheral devices.
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 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 a Keno Licence.
Memory	An area of a computing device used to store data and/or instructions.
Network Policy Document	A document describing the end-to-end network topology of a Keno System which is the responsibility of the Licensee to prepare as part of its submission to the Commission when obtaining approval for a Keno System.
Online distribution methods	The ability for a customer to purchase entries in a Keno game, and to receive payments via online access to a Keno System via an access application operating on a user device (such as a personal computer or mobile device).
PCI	Payment Card Industry
PCI compliant	Indicates compliance with the Payment Card Industry Data Security Standards, as set by the PCI Security Standard Council.
Player Account	A registered account in a Keno System where a verified and authorised person may transfer funds between a debit account in an Australian financial institution and that Keno System. A Player Account may be used for purchasing entries in Keno Games and any winning outcomes subsequently credited to that account.
Prorating	Means the reduction in the value of expected prizes payable as per the rules of the game in circumstances of exceeding maximum prize limits.
RAM	Random Access Memory - the storage facility used by the Central Processing Unit 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 a 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.
Significant Event	In regard to a 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 this Standard.
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 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 of Manufacturers, Suppliers and Testers as described in Chapter 3, Part 4, Division 7 of the Act, that operates an Accredited Testing Facility.
UPS	Uninterruptible Power Supply (a no-break mains power supply including battery backup equipment).
VGCCC	Victorian Gambling & Casino Control Commission
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, or cadastrally separate sites

2 Foreword

This chapter introduces the background to a Keno Technical Standard.

2.1 Keno Technical Standard Evolution

- 2.1.1 A Keno Technical Standard is intended to provide Keno Licensees with a set of technical standards and guidelines that must be met for the implementation of a Keno System in Victoria.
- 2.1.2 Between April 2012 and April 2022, a single Keno Licensee operated in Victoria and Technical Standards were originally issued in November 2011. A minor revision was issued in June 2017.
- 2.1.3 In 2019, the Minister for Gaming issued a Request for Expression of Interest (EOI) in the grant of a Keno Licence for post 15 April 2022. The EOI contemplated options for Keno licensing including single source, long term licensee or multiple licensees.
- 2.1.4 The EOI also introduced the potential for online distribution of Keno – a capability not permitted in Victoria until 15 April 2022.
- 2.1.5 To support the new Keno licence period, the VGCCC Keno Technical Standard has been revised. The changes are intended to ensure relevance of the Standards over the licence period and acknowledge the potential for improvement and efficiencies in related technologies and general online customer participation and digital payment technologies.
- 2.1.6 It is emphasized that these Standards are not intended to prescribe or specify any particular technology, method or algorithm. The intent is to allow a wide range of methods to be used to conform to the Standard, while at the same time, enabling the introduction of evolving technologies to be proposed by Licensees from time to time.

3 Introduction

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

3.1 General Information

- 3.1.1 A Keno Technical Standard contains the related technical system requirements for a Keno System operated by the holder of a Victorian Keno Licence. The standard is a technical standard made by the Commission pursuant to section 10.1.5A of the Gambling Regulation Act 2003 (the Act).
- 3.1.2 This document is to be used by a Licensee and a Tester to evaluate the system for compliance with a Keno System requirements, or to evaluate changes to a previously approved system for approval.
- 3.1.3 This document is also to be used by the Victorian Gambling and Casino Control Commission (VGCCC) to evaluate compliance by a Licensee with a Keno Licence and Related Agreement(s), and to evaluate changes to a previously approved Keno System, in accordance with section 6A.2.5 of 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 a Licensee refer to an entity licensed to conduct a Keno activity identified by its Licence and Related Agreement(s).
- 3.1.5 Requirements for the VGCCC's revenue audit, compliance verification audit, disaster recovery, and ICT service management are also defined in this document.

The Act

- 3.1.6 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).

Objectives

- 3.1.7 The VGCCC 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 approved Keno Rules for the associated Keno activity,
 - ii) the system is fair to players,
 - iii) revenue and taxable amounts are calculated, recorded and reported accurately for sales initiated in Victoria,
 - iv) keno draws are generated securely and randomly in an unpredictable manner
 - v) the system operates in a manner that is auditable, reliable and secure,
 - vi) all parties receive their correct entitlement,
 - vii) distribution of Keno via online means includes adequate provisions to verify customer identity and account security, and
 - viii) minimises the potential for harm from gambling and provides support to player protection measures.
- 3.1.8 Matters arising from the testing of a Keno System that have not been addressed in this document will be resolved at the sole discretion of the VGCCC as part of the approval process. In considering

any new technology or omissions, the VGCCC may take into account advice on such matters from the Licensee, or a Tester, or both.

Document Scope

- 3.1.9 The requirements in this document apply to a Keno System to be operated by a Licensee according to a Keno Licence and Related Agreement(s).
- 3.1.10 A reference to a Keno Licensee in this document is a reference to a holder of a Victorian Keno Licence.

Location of Keno System

- 3.1.11 A Keno System (including the Host Computer site and Disaster Recovery site and associated data facilities) must be located in Australia. Keno venues must be located in Victoria.
- 3.1.12 Subject to the provisions of its Keno Licence, a Keno System operated by a Keno Licensee may be permitted to distribute Keno games via online distribution methods.
- 3.1.13 Storage of Keno System data must be located in Australia, unless otherwise approved by VGCCC.

Keno Sales Outside of Victoria

- 3.1.14 Where a Keno System incorporates the online distribution of Keno, it must be capable of identifying, recording and reporting Keno purchases that are initiated outside of Victoria separately from purchases initiated within Victoria.

3.2 Keno System Design

- 3.2.1 The VGCCC expects that a Keno System will consist of the following Components:
 - i) A main host computer system, which provides Keno as a rapid draw lottery;
 - 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) Subject to the provisions of a Keno Licence, application software made available to customers to download to remote devices for the purposes of online distribution of Keno games;
 - v) Operator driven Keno Terminals used for selling, paying and cancelling Entries and other transactions;
 - vi) Optional self-service Keno Terminals in venues; and
 - vii) 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 a Keno System and equipment operate as approved by the VGCCC, 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:
 - a) a service support function which incorporates:
 - i) incident management;
 - ii) problem management;

- iii) Configuration Management
- iv) change management;
- v) release management;
- b) a Service delivery function which incorporates:
 - i) availability management;
 - ii) capacity management;
 - iii) service level management;
 - iv) service continuity management;
- c) security management
 - i) the Licensee must establish and maintain Information Security Management Systems that meet ISO/IEC 27001:2013 or equivalent standard
- d) ICT infrastructure management (hardware and software)
 - i) Design, deployment and operational management of ICT equipment and software in the provision of a Keno System as approved by the Commission
- e) application management
 - i) the ongoing management of all Keno System applications which will include but not limited to: designing, testing, operating, improving and support.

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

- 3.3.2 Within the ICT Service Management Framework, the Licensee must establish and maintain Quality Management Systems¹ that meet ISO 9000² or an equivalent standard.
- 3.3.3 Within the ICT Service Management Framework, the Licensee must establish and maintain Information Security Management Systems³ that meet ISO 27000⁴ or an equivalent standard.
- 3.3.4 The Licensee must establish policies, procedures and standards for data governance.
- 3.3.5 The Licensee must establish policies, procedures and standards for cyber security set out in the Australian Government Information Security Manual (ISM) or equivalent.
- 3.3.6 The Licensee must establish processes and controls for patch management of the Keno System.
- 3.3.7 The Licensee must establish processes and controls for anti-virus management of the Keno System.

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 VGCCC.

¹ The organisation 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

- 3.4.2 When a Keno 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.

System Performance Standards

- 3.4.3 A Keno System must be capable of meeting the relevant performance standards set out in a Keno Licence and Related Agreement(s).
- 3.4.4 Communication systems forming part of, or used in association or connection with, a Keno System must be capable of meeting the performance standards set out in the Licence and Related Agreement(s).
- 3.4.5 A Keno System must operate only as approved and in accordance with the requirements of any standards, specifications or conditions determined by the VGCCC.
- 3.4.6 A Keno System must be capable at all times of determining whether all Components of a 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 A Keno System operated by a Keno Licensee under the provisions of a Victorian Keno Licence must be approved by the VGCCC.
- 3.5.2 Approval must be obtained from the VGCCC 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 VGCCC, before such equipment becomes part of a Keno System.
- 3.5.3 Each Component of any one hardware revision level shall be identical.
- 3.5.4 A Component of a Keno System may have multiple suppliers of major assemblies, but approval must be obtained from the VGCCC for each Component from each supplier. Off the shelf and custom-built Components of a 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 requirements for Central Components of a Keno System that must be followed.

4.1 Keno System Requirements

4.1.1 VGCCC 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 VGCCC.

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

- i. Visibility of system status, keeping operators and 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 a Keno System shall be designed in consideration of best practice standards of accessibility.

Electromagnetic interference (EMI), Electromagnetic compatibility (EMC) Electrostatic Interference & Safety

4.1.4 The Standard reminds the Manufacturers of their obligatory requirements to ensure that the Keno System and associated equipment within the Keno System environment complies with prevailing statutory and applicable EMI, EMC, Electrostatic Interference and Safety Standards administered by relevant regulatory bodies through International and/or Australian/New Zealand or local standards.

4.1.5 Except where specifically identified in the Standard, testing is not directed at health or safety matters or at ensuring legislative requirements administered by other regulatory bodies such as for electrical safety and of radio frequency emission, etc. These matters are the domain and responsibility of the manufacturer, purchaser and operator of the equipment. Each of these parties is required to assure themselves of such matters.

4.2 Licensee-operated Central Keno System Environment

Physical Security

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

4.2.2 Access to the data centre must be secured and controlled.

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

4.2.4 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

4.2.5 All machinery, equipment and computer systems within the central components of a Keno System computer room(s) environment must be supported by an environmental monitoring system.

4.2.6 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 a Keno System and to automatically alert if these conditions are not met.

Power Supply

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

4.2.8 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.

- 4.2.9 If the supply of mains power to the central components of a Keno System 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 components of a Keno System environment.
- 4.2.10 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 VGCCC, when the VGCCC conducts an audit.
- 4.2.11 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 VGCCC, and the VGCCC may be in attendance at any test.

Uninterruptible Power Supply (UPS)

- 4.2.12 The computer, security and telecommunication systems within or contributing to the central components of a Keno System must be protected against power fluctuations and temporary loss by installation of a UPS or other such device.
- 4.2.13 The UPS must provide sufficient supply to support the central components of a 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.
- 4.2.14 All machinery, equipment and computer systems situated in the central components of a Keno System computer room must be earthed via the UPS.

Stand-by Generator

- 4.2.15 The central components of a 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 components of a Keno System and facilities for a period of not less than 24 hours.

Emergency Lighting

- 4.2.16 The central components of a 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.

4.3 Cloud-based computing environment for a Keno System

- 4.3.1 The VGCCC must approve all Keno System data storage and proposed cloud computing.
- 4.3.2 The VGCCC may also approve an application from a Licensee to operate their Keno System in a Cloud Computing Environment.
- 4.3.3 Applications to utilise a Cloud Computing Environment must include
 - a) a description of the cloud service model (e.g. Software as a Service, Platform as a Service, or Infrastructure as a Service);
 - b) a description of the proposed cloud model (e.g. Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud) and sufficient details of the cloud owner and operator to support the application;
 - c) details of which applications of a Keno System are intended to operate in a cloud environment;

- d) details of a risk assessment conducted by the Licensee into the cloud service provider and the cloud environment; and
- e) any other information requested by the VGCCC in consideration of the application.

4.3.4 In addition, refer to the VGCCC Regulatory Framework and Application process for requirements on cloud computing.

4.4 Help Desk facility

4.4.1 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.

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

4.4.3 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.

4.4.4 All calls to the Help Desk must be logged and the log made available to the VGCCC 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.

4.5 A Keno System

4.5.1 A Keno System consists of components that enable the Keno business to operate in a secure environment and meet the legislative requirements and the licensee's obligations under the relevant License they hold.

4.5.2 The VGCCC defines the components of a Keno System into the following categories, each with differing regulatory requirements:

Baseline Components

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

- Operations and monitoring of all Keno activities and devices, and related transactions to and from the devices
- Any associated system-based Keno activities

- Functions that are related to critical data
- Functions required by regulatory and/or government bodies
- Primary source of storing the critical data in relation to the Keno activities, and
- Structured reporting in relation to the ongoing monitoring of Keno activities.

First Tier Non-Baseline Components

Software and hardware that are directly interfacing with baseline components.

Second Tier Non-Baseline Components

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

- 4.5.3 A Keno System must operate in accordance with a Keno Rules as consented to by the VGCCC and any regulations associated with operating a Keno Business.
- 4.5.4 VGCCC approval must be obtained for the software configuration (baseline) of a Keno System.
- 4.5.5 The Tester's assessment will evaluate the software configuration for reliability, recovery, audit ability, redundancy and security.
- 4.5.6 The VGCCC must maintain ongoing visibility of the end to end Keno System, including all components outlined above (section 4.5.2).
- 4.5.7 A Licensee must ensure that any additions or deletions to a Keno System components are appropriately classified into one of the abovementioned categories, and the appropriate regulatory response is initiated, i.e.; approval of baselined components or notification of a new First Tier non-baseline components.
- 4.5.8 It is recommended that if the classification in relation to any changes to a Keno System is contentious, the Licensee should actively consult with the VGCCC, prior to development and/or implementation of the changes, to ensure the correct classification is made and the appropriate regulatory action is initiated.
- 4.5.9 Should the Licensee seek the VGCCC's advice on the appropriate classification of any changes to a Keno System, the VGCCC may seek that a report from an Authorised Testing Facility (ATF) is provided to support the request, and certifies the classification made by the Licensee.
- 4.5.10 If deemed that the Licensee has incorrectly classified any changes to a Keno System, the VGCCC could instruct the Licensee to reclassify the change which may require further development, cost and rework by the Licensee. Further action may also be considered for operating an unapproved system should the Commission determine that components should have been baselined and therefore subject to regulatory approval before operating.

System Document

- 4.5.11 The Licensee must prepare and maintain a System Document and submit to the VGCCC on an annual basis.
- 4.5.12 The System Document must include at least the following:
- All baseline components;
 - All first and second tier non-baseline components;

- iii. A system network document, which clearly identifies the core areas of a 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;
 - iv. The procedure for handling system changes in general;
 - v. The procedure for handling Emergency Changes;
 - vi. The procedure for maintaining the System Document, including any Emergency Changes.
 - vii. Any other operation or procedure that is relevant to securing control of the system.
 - viii. Any changes implemented in the last 12 months, or in comparison to the last Keno System document; and
 - ix. The method and mechanisms used to verify that a Keno System is operating in an approved state;
- 4.5.13 Emergency Changes to a Keno System must be notified to the VGCCC 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. A 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 VGCCC final approval are required for all Emergency Changes as soon as practical after the change has been applied.
- 4.5.14 A Tester recommendation is required for all changes to the system document, including any Emergency Changes.
- 4.5.15 VGCCC approval, having regard to any relevant Tester recommendation, must be obtained for any changes to the baseline, including any Emergency Changes.
- 4.5.16 In order to establish a baseline, an agreement must be reached with the VGCCC regarding the directories in which application files will be located on the central components of a 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.
- 4.5.17 A Keno System must have a method to verify the baseline components 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 baseline components residing on storage devices or in the memory of a Keno System are only executable for the Keno System.
- 4.5.18 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 VGCCC) are checked regularly to ensure that unauthorised activities are not taking place on the system.

Keno System Software Procedures

- 4.5.19 The Licensee must establish and maintain policies, procedures and standards in accordance with the requirement at 3.3 of this document.
- 4.5.20 The operational control of a Keno System must be administered in accordance with adequate internal control policies, procedures and standards.
- 4.5.21 Only approved application files within the baseline may reside on storage devices or in the memory of the Keno System computers.

Financial Transactions and Records in Australian Dollars

- 4.5.22 All financial transactions, records and reports within, or generated by, a Keno System must be in Australian Dollar currency.
- 4.5.23 If its Licence provisions permit customer or Player Accounts transactions in any other currency unit, a Licensee is responsible for cost and risk associated with conversion from and to Australian dollars and this must take place in corporate systems outside the Keno System baseline.

4.6 Keno System Software Quality

Software Version Control

- 4.6.1 All software for all Components of a Keno System must be maintained under an appropriate software version control system or mechanism.

Software Verification During Development

- 4.6.2 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 VGCCC for approval and live operation.

4.6.3 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 a Keno System.

Central Logging of Information

- 4.6.4 All security logs must be regularly reviewed, and preventative or corrective actions must be undertaken by the Licensee in a timely manner.
- 4.6.5 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

- 4.6.6 The Licensee must securely maintain a register of all dividend money that has not been claimed as required by relevant legislation.
- 4.6.7 The serial numbers or other access method for 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.

- 4.6.8 Expired unclaimed ticket data stored on or extracted from the system must be adequately secured and controlled including, but not limited to ensuring:
- i. Data integrity
 - ii. Data confidentiality
 - iii. Data availability
 - iv. Safe and secure purging of data when required

Financial Summary Reporting

- 4.6.9 A report which details the financial summary for each Keno Terminal for each Keno Venue, total for all terminals, and an aggregate financial summary for all Keno games distributed via online methods is to be provided daily (or any period/frequency determined by the VGCCC) to the VGCCC.
- 4.6.10 The content and format of the daily (or any period/frequency determined by the VGCCC) financial report must be agreed with the VGCCC, but at a minimum, the following information must be included:
- i. Transactions on and current amount of the prize fund;
 - ii. Sales made in Victoria;
 - iii. Sales made outside of Victoria;
 - iv. Cancels;
 - v. Pays;
 - vi. Voucher sales and redemptions;
 - vii. Keno Licensee and Keno Licensee Agents payments;
 - viii. Jackpot transactions;
 - ix. Theoretical liability;
 - x. Government share of revenue; and
 - xi. Account deposits and withdrawals.

Program Storage Devices

- 4.6.11 VGCCC approval must be obtained for the method of program storage and the method(s) for modifying programs for all devices.
- 4.6.12 Any Component of a 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

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

4.7 Significant Events

Generation of Significant Events

- 4.7.1 The Licensee must establish and maintain policies, procedures and standards for reporting Significant Events to the VGCCC in a format to be determined by the VGCCC, including but not limited to:
- i. Situations where the system is incapable of supporting a Keno Rules;
 - ii. System failures;
 - iii. Instances where there has been any form of unauthorised access to any Component of a 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 payment creation and processing; and
 - xv. Changes to prize tables, jackpot parameters or prorating parameters.
- 4.7.2 Where this document states that a Keno System must detect and record Significant Events, it does not imply a particular implementation.

Storage of Significant Events

- 4.7.3 The Significant Events prescribed by the VGCCC, regardless of the source of these events, are to be stored at the Licensee's premises.
- 4.7.4 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.
- 4.7.5 Significant Events may also be stored in subsidiary points of a Keno System.

Recovery of Significant Events

- 4.7.6 The system must be designed such that in the event of the failure of the central system database it is possible to electronically recover the Significant Events using a method that ensures no Significant Events are lost.

4.8 End of Keno Game Processing

Keno Game Number Increment

- 4.8.1 When a 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.
- 4.8.2 Any Entries placed, including those that might have been "in transit" to the central components of a Keno System, are to be associated with the new Keno Game number, not the old.

Late Cancels

- 4.8.3 The Licensee may apply to the VGCCC for a scheme to facilitate late cancels.
- 4.8.4 A Keno System is to prevent Late Cancels once the first number is drawn.

Entries During a Draw

- 4.8.5 The VGCCC may approve restricted Entries during the number drawing sequence, defined to be the time from Stop Sell⁵ to Confirm Results⁶, which includes the number drawing selection and end of Keno Game processing.
- 4.8.6 Entry restrictions during a draw are as follows:
- i. Selling is permissible if a 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 a 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 a Keno Game which is being completed; i.e. all forward games must have been finished before a Keno Game which is currently being drawn or processed. The VGCCC 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

- 4.8.7 Once all results are received from the RNG and results have been confirmed, a 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.

⁵ Stop Sell means the point of cessation of selling tickets in the current game

⁶ Confirm Results means the point at which results from the current game have been confirmed

- ii. If jackpots are active, a 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 a Keno Rules and the jackpots that have been won must be reset as per a Keno Rules. A Significant Event for the jackpot(s) won must be generated and reported to the VGCCC in accordance with 4.7 of this document.
- iii. If prorating of winners is specified in a Keno Rules, a Keno System must scan all active Entries for winners that might qualify for prorating (for example, large wins) as per a Keno Rules. If the sum of these prizes exceeds a limit as specified by a 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 a Keno Rules. A Significant Event for the prorating must be generated and reported to the VGCCC in accordance with 4.5 of this document.
- iv. A 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,

4.9 Keno System Security

- 4.9.1 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.
- 4.9.2 The operating system of the computer's application files and database must provide comprehensive access security.
- 4.9.3 The Licensee must establish policies, procedures and standards for the use of passwords or equivalent based on current best practices, which should 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 enforced password changes when required 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.
- 4.9.4 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.
- 4.9.5 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.
- 4.9.6 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.
- 4.9.7 The Keno system's storage of passwords must comply with the Licensee's security policies, procedures and standards and must provide for an encrypted, non-reversible form.
- 4.9.8 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 VGCCC.
- 4.9.9 The Licensee must ensure that access to specific functions within a 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 VGCCC.
- 4.9.10 The Licensee must develop and maintain policies and operating procedures designed to prevent hacking or unauthorised access to its Keno System.
- 4.9.11 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 (or recommended best industry practice agreed by VGCCC) and provide a written report of its findings. This report must be provided to the VGCCC 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.
- 4.9.12 The Licensee must establish policies, procedures and standards for the management and usage of administrative, generic, service and system accounts.

Auditability of the Keno System

- 4.9.13 The Licensee will be subject to regular compliance and system audits by the Commission or an Inspector.
- 4.9.14 The system audit will assess the security and controls over the system to ensure that the system is operating as approved by the Commission and integrity of Keno System and data are maintained at all times.
- 4.9.15 The scope of the audits includes but is not limited to:
- a) logical access security and control such as user access creation, user and access privileges reviews, generic accounts security and controls, remote access control and management
 - b) physical and environment security such as data centre access controls, RNG security and control

- c) system integrity such as approved components Baseline verification for compliance, source code integrity, regular monitoring of critical activities of the system and its components with preventive, detective, and corrective controls in place
- d) data and information security and integrity such as database security and control, financial data integrity, customer data and information integrity
- e) game resulting and outcome integrity such as security and controls of draw process and procedures, RNG, unclaimed keno tickets
- f) networks and communications security such as regular Network Policy Document reviews, prevention, detection and correction measures for relevant security breaches
- g) software, Hardware and network change management and deployment such as emergency change and Configuration Management
- h) problem and incident management including significant events management
- i) system availability such as backup security and controls by regular testing of retrieval and restore from backup devices, storage management records
- j) business continuity management such as disaster recovery and business continuity planning, testing and documentation
- k) asset management such inventory management of approved components
- l) system interfaces and peripheral equipment integrity
- m) accountability maintained by appropriate segregation of duties
- n) adequate audit trail maintained for accountability, reconstruction, intrusion detection, problem detection
- o) system and audit log monitoring including appropriate procedures for follow-up and corrective action
- p) adequate audit trail and logs kept to help in auditing through the computer as for customer complaints and investigation
- q) availability of adequate policies, procedures and standards, which are regularly followed, maintained and kept up to date.

4.10 Keno System Recovery

Transaction Logging

- 4.10.1 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.
- 4.10.2 For transaction logging the Licensee must ensure that:
 - i. The central components of a 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 VGCCC; and
 - iv. All adjustments or modifications to the transactions (and unclaimed monies or accounts) must be recorded with a Keno System operator's user ID (and time/date-stamp).
- 4.10.3 All transactions and events are to be serially written to the log in the order that they occur.
- 4.10.4 There must be no possible means of "adding records" to the middle of the log or "writing over" existing records.

4.10.5 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

4.10.6 All log records must have a standard format, for which approval must be obtained from the VGCCC, 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 a Keno System for which the transaction/event occurred;
- iv. A unique event identifier which defines the transaction/event;
- v. A Keno Game number when the transaction/event occurred, where appropriate; and
- vi. Any relevant data that is associated with the transaction/event.

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

Logging of Keno Entries

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

- i. Starting game number;
- ii. Where a 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 a 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

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

4.10.10 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).

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

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

4.10.13 The Licensee must establish and maintain a comprehensive disaster recovery test plan, including a schedule for testing, , which must be supplied to the VGCCC upon request and conduct disaster recovery testing in accordance with the plan.

In the event of a disaster, for example, a fire, there must be a method of ensuring that all data and information related to a 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.

- 4.10.14 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.
- 4.10.15 There must be periodic back-ups (at least daily) of the variable database files on the central components of a Keno System's storage devices.

System Data Recovery

- 4.10.16 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.
- 4.10.17 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 VGCCC.
- 4.10.18 Backup data must be secured and access to backup data is controlled.
- 4.10.19 Retrieval and restoration of backup data must be performed in a secured and controlled manner and environment.
- 4.10.20 Retrieval and restoration of critical data used for any other purpose such as testing or big data initiatives must require VGCCC approval. VGCCC may require the data to be obfuscated and encrypted.

Central Site Failure Modes and Recovery

- 4.10.21 Following any failure, it must be possible to restore the state of a Keno System and its database(s) without losing data.
- 4.10.22 All backup or stand-by systems should be tested regularly to ensure the timely support of the systems.
- 4.10.23 Some typical tests that may be required by the VGCCC to test compliance with this and other sections of a 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.).

4.11 Data Security

Encryption of Stored Data

- 4.11.1 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 Security Manual (ISM)⁷.
- 4.11.2 As a minimum, the following information classes must be encrypted in a non-reversible form for storage and use:
- i. PINs; and
 - ii. Passwords.
- 4.11.3 As a minimum, the following information classes must be encrypted (reversible) for storage for recovery purposes:
- i. Encryption/Decryption Keys;
 - 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 VGCCC, and critical fields such as authentication codes.

PIN and Password Management

- 4.11.4 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 VGCCC.
- 4.11.5 The storage of PINs or passwords 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 or password data, he/she must not be able to reconstruct the PIN or password from that data even if the PIN or password creation algorithm is known.

4.12 Keno System Integrity

- 4.12.1 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.
- 4.12.2 The Keno System must be able to log an audit trail of all manual updates to the database.
- 4.12.3 VGCCC approval must be obtained for the configuration management plan and the configuration of the central components of a Keno System.
- 4.12.4 The Tester will evaluate the configuration for operational integrity as well as recoverability, redundancy and security.

Security of Event Logs

- 4.12.5 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

⁷ <https://www.asd.gov.au/infosec/ism/>

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

- 4.12.6 Data files and databases that contain vital information must be duplicated for integrity, availability, and reliability.
- 4.12.7 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

- 4.12.8 Details of the VGCCC's reporting requirements will be provided to the Licensee by the VGCCC.

VGCCC Required Reports

- 4.12.9 As a minimum, financial information by event conducted must be made available to the VGCCC in a format specified by the VGCCC that is compatible for processing by the VGCCC's systems.
- 4.12.10 Reports supplied to the VGCCC must be complete, comprehensive, accurate, clearly delineated, and available in electronic format.

System Integration

- 4.12.11 The VGCCC may approve the integration of sub-systems or utilities with a 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.
- 4.12.12 The real-time monitoring and inspection facility described in 4.12.11 of this document is not required to be a Component of this approval process.
- 4.12.13 The integration of the central components of a Keno System with sub-systems or utilities must be described in the configuration management plan.

Access by the VGCCC

- 4.12.14 Keno system design and operation must facilitate the exercise of powers by VGCCC Inspectors as provided for under legislation. The Licensee, at the direction of the VGCCC or an Inspector appointed by the VGCCC, must provide access to the information on the Keno System, including but not limited to, application and database at any time.
- 4.12.15 The central components of a Keno System software must provide tools and mechanisms to:
 - i. Examine Significant Events;
 - ii. Examine data; and

iii. Verify the approved system baseline.

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

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

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

Link to VGCCC Computing Facilities

4.12.19 The real-time monitoring and inspection facility described in 4.12.14 of this document must include a secure electronic link from the Licensee's Central Keno System site to the VGCCC's computer facilities.

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

4.12.21 The provision of financial data and the reports described in 4.10.8 of this document will be provided in a method and frequency deemed acceptable by VGCCC, including the use of alternative tools (including off-the-shelf tools) without requiring integration into the real-time monitoring and inspection facility. .

4.12.22 The data link between the VGCCC 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

4.12.23 Facilities for VGCCC 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 a Keno System is on- line;
- v. Facilities to support an inspector working together with an inspector in the field;
- vi. On request, 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 VGCCC's premises; and
- x. Provision of licensee technicians on request from the VGCCC to assist VGCCC Inspector's in the conduct of technical compliance.

4.13 Keno Terminal Hardware

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

- 4.13.2 A 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.
- 4.13.3 All banknote acceptance devices used in Keno Terminals must be constructed in a manner that protects against vandalism, abuse or fraudulent activity. As a guide the following should be addressed:
- ability to prevent manipulation by the insertion of foreign objects into the banknote input system;
 - ability to deliver a banknote to the banknote storage area (e.g. receptacle), and
 - it must not be possible to disable any validation feature.

4.14 Keno Terminal Functions

- 4.14.1 VGCCC approval must be obtained for all Keno Terminal functions pertinent to Keno Games.
- 4.14.2 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 a Keno Games.
- 4.14.3 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.
- 4.14.4 VGCCC approval must be obtained for the method and security of communications to and from a Keno Terminal.

4.15 Customer application software for online Keno Distribution

- 4.15.1 Subject to the provisions of its Keno Licence, a Licensee may distribute Keno online over the internet and similar communications channels via application software installed on mobile devices or personal computers.
- 4.15.2 Subject to provisions of its Keno Licence, a Licensee's application software that enables members of the public to observe Keno game draws, review past Keno game results, participate in marketing activities and promotions or establish a Player Account for the purpose of online purchases of Keno games must:
- a) comply with the Act and regulations;
 - b) include clear statements that enable a customer to understand which jurisdiction a Keno game is licensed in, and whom it is regulated by;
 - c) provide contact details of a Keno Licensee and the VGCCC for customers connected to the Victorian Keno game; and
 - d) provide easily accessible terms and conditions and general information in a clear and intelligible manner;

4.15.3 Subject to provisions of its Keno Licence, a Licensee's application software that enables holders of a Player Account to purchase entries to a Keno game must:

- a) Make available a display of the result of every game in which the player participates for a reasonable period of time;

- b) provide a means for an account holder to view past game entries and results, and, if applicable to that account holder, to view future game entries;
- c) display information about the game result in sufficient detail for the player to determine whether they have won or lost and the value of any winnings; and
- d) display Player Account balance in currency value (dollars and cents).

5 Network and Communications

This chapter sets out a 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 a Keno System at a Keno Venue, and between a Keno Venue and a Central Keno System site (but not necessarily within the central components of a 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. The Licensee must provide notification to VGCCC of any software or tools that are able to decrypt or reveal critical data such as ticket serial numbers.
 - v. 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 Keno System.
- vi. 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 VGCCC.

Encryption Algorithm

5.1.5 The following are encryption characteristics that must be considered:

- i. Encryption algorithms are to be demonstrably secure against cryptanalytic attacks⁸ and must confirm to industry standards;
- ii. The minimum width (size) for encryption keys must conform to industry standard encryption;
- 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

5.1.6 The following are authentication characteristics that must 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 Key algorithms to be used to provide Cryptographic Data Security which must conform to industry standard encryption and authentication structures.

5.2 Communications Requirements

Data Communications

- 5.2.1 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.
- 5.2.2 The VGCCC will only approve a protocol if it is confident that the devices implementing the protocol will fully comply with the requirements of this document.
- 5.2.3 All Components of a Keno System must be able to “gracefully” handle a range of simple failures.

⁸ Cryptanalytic attack is the method for obtaining the meaning of encrypted information, without access to the encryption key, in an unauthorised way

- 5.2.4 A Keno System Equipment must be recoverable to the point of failure following an interruption.
- 5.2.5 Only approved data communication control functions of a Keno System should be implemented. These control functions must be clearly specified in the System documentation.

5.3 Network Requirements

- 5.3.1 This section describes the VGCCC'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 VGCCC as to be under baseline control, and must be described by a Keno Licensee in a configuration management plan.
- 5.3.3 The Licensee must ensure access to the network devices are secured and controlled.

Network Baseline

- 5.3.4 During the approval stage of a system network, the VGCCC 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.
- 5.3.5 The Network Policy Document (NPD) must be established and maintained by a 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.
- 5.3.6 The Licensee must have in place an approved NPD which details the approved state of a Keno System network, what changes must be approved by the VGCCC and what changes require notification to the VGCCC.
- 5.3.7 The NPD must be reviewed and evaluated by a Tester and approved by VGCCC.
- 5.3.8 The Licensee must establish internal processes to ensure ongoing compliance with the approved NPD.

Physical Requirements

- 5.3.9 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 a Keno System must be protected by a filtered, dedicated power circuit.
- 5.3.10 Cabling used in production networks must be protected against unauthorised physical access and malicious damage.

Network Documentation

- 5.3.11 All cabling and devices must be clearly labelled by function.
- 5.3.12 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.
- 5.3.13 Connection of External Devices to Networks Inside a Baseline Envelope
- 5.3.14 Unused ports on network devices and network control devices inside and on the boundary of the baseline envelope must be disabled.
- 5.3.15 The facilities for plug and play10 installation of unregulated devices must be disabled.

- 5.3.16 Host computer systems, network devices and network control devices within 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.
- 5.3.17 Configuration changes to all devices within the baseline envelope must be protected by encrypted passwords. Password protection policies, procedures and standards must exist and be implemented by a Keno Licensee, including provision of prevention, detection and correction measures for non-compliance.
- 5.3.18 An audit log must be maintained for all changes to the configuration of any network devices within 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.
- 5.3.19 At the central components of a 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

- 5.3.20 There must be no loss of information due to a failure of a redundant communications network within a baseline envelope.
- 5.3.21 All information traversing the network between remote equipment and the central components of a Keno System host must be recoverable once communications are restored.

Communications between Separate Baseline Envelopes

- 5.3.22 Information flowing between different baseline envelopes must be subject to authentication and encryption, unless the VGCCC has approved an exception that the intervening network is physically and adequately secure and under the complete control of the Licensee.
- 5.3.23 WAN communication links are deemed to be outside a baseline envelope and VGCCC approval must be obtained for any exceptions.
- 5.3.24 There is to be no loss of information due to a failure of a redundant communications network between baseline envelopes.
- 5.3.25 Communication between devices in separate baseline envelopes must be protected and 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 VGCCC 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 VGCCC 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 components of a 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 VGCCC, and VGCCC approval must be obtained for any exceptions.

Monitoring Systems and Network Management Systems

- 5.3.36 VGCCC approval must be obtained for any applications or utilities that enable monitoring of Components of a 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 VGCCC 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 VGCCC. 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 A Keno System, at the point where it is connected to the Internet service provider, must incorporate a DMZ⁹like 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 VGCCC 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 VGCCC provided that there are appropriate additional security measures in place, which meet the standards set out for wireless communication in the Australian Government Information Technology Security Manual (ISM)¹⁰ 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 components of a Keno System.
- 5.4.3 The wireless access point must be physically positioned so that it is not easily accessible by unauthorised individuals.
- 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,

⁹ 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

¹⁰ <https://www.asd.gov.au/infosec/ism/>

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 VGCCC will consider performance and availability before granting approval to the use of wireless communication.

6 Testing Requirements

This chapter sets out Keno System requirements that must be followed for operations in Victoria.

6.1 Inspection and Testing

- 6.1.1 The VGCCC 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 quality¹¹assurance 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 VGCCC.
- 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 a 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;

¹¹ The methods an organisation puts in place to ensure reliable quality control

- 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 a 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 VGCCC accordingly.

Test Environment

- 6.1.6 The Licensee must ensure that upgrades to machinery, equipment and computer systems making up a 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 VGCCC.
- 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 components of a Keno System for resilience, recoverability and continuity of service, including but not limited to conditions for:
- i. Failure of the central components of a Keno System power supply;
 - ii. Total power failure of the central components of a 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 a 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 Document and the Network Policy Document for future approval.

Associated Systems Requirements

- 6.2.3 All the systems associated with a Keno System are required to be tested for reliability in processing and delivering all transactions for a 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 tester/VGCCC for testing/approval, at the minimum, must include the following:
 - i. Background of a 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 a Keno System;
 - v. Description of all networks within a Keno System;
 - vi. Description of any proposed cloud computer environments and suppliers/operators thereof;
 - vii. Tester recommendation regarding a Keno System in accordance with above requirements;
 - viii. The Licensee's comments on any conditions included in the Tester's recommendation;
 - ix. List of all software versions and associated Hash Results;
 - x. List of all relevant hardware and operating systems – product names, models and versions;
 - xi. Associated systems that are connected to a Keno System;
 - xii. A Keno System document; and

- xiii. A Network Policy Document (if applicable).

Approval and Notification Requirements

- 6.2.6 Any changes to a Keno System components that have been defined by the Licensee to be within the baseline envelope must have VGCCC approval before being activated.
- 6.2.7 VGCCC approval is not required for the components outside the baseline envelope (non-baselined components), however the Licensee must notify the VGCCC within 14 days of installing a new First Tier non- baseline component on a Keno System.

Environmental Testing

- 6.2.8 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.
- 6.2.9 The VGCCC requires the equipment to run within the equipment's own environmental specifications.

7 Player Accounts

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

7.1 Player Account capability

- 7.1.1 Subject to provisions of its Keno Licence, a Licensee may be permitted to offer account based Keno activities to players who are pre-registered and hold a Player Account with the Licensee.
- 7.1.2 A 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 who have not self-excluded from Keno, are permitted to create a Player Account.
- 7.2.2 A person must not have more than one Player Account per Licensee.
- 7.2.3 The Licensee must securely maintain a register of Player Account verifications.
- 7.2.4 Upon registration in a Keno System, each player must be allocated a unique identifier to enable identification of the appropriate player and account details by a Keno System each time a player commences a session.
- 7.2.5 At the time a registration for a Player Account is accepted by a Keno System, the Player Account holder must be required to set their own account password or player identification number (PIN) that must be used before access to funds in a Player Account can be made.
- 7.2.6 The Licensee must establish and implement a secure process for Player Account holders to reset their PINs or password.
- 7.2.7 The Licensee must securely maintain a register of Player Accounts.
- 7.2.8 The use of other financial instruments or payment methods to be associated with a Player Account must be specifically permitted under approved Keno Rules.
- 7.2.9 A Keno System must facilitate the deactivation of a Player Account and re-registration.
- 7.2.10 A new Player Account for a person must not be created if the deactivation reason for a previous Player Account indicates that the person must not be permitted to establish another Player Account.
- 7.2.11 A 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 and maintained by the Licensee in respect of a Player account must be kept confidential by the Licensee as required under the Licence and Ancillary Agreement(s), except where the release of that information is required by law or approved by the registered Player.

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

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

- 7.3.2 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 a 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 debit card transaction must not be available for the purpose of placing a Keno Entry until such time as the funds are confirmed from the financial institution. The financial institution 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 PINs or password entry, must be made before withdrawal of monies held in a Player Account by a Keno System can be made.
- 7.4.5 Subject to any restrictions that may be legitimately apply (i.e. ongoing criminal investigation or restrictions imposed by the Licensee), a Player Account holder must be able to withdraw funds from their account at any time.
- 7.4.6 Inactive Player Accounts holding monies held in the system must be protected against forms of illicit access or removal.
- 7.4.7 All transactions involving monies are to be treated as vital information to be recovered by a Keno System in the event of a failure.
- 7.4.8 Personal information of a sensitive nature must only be stored in an encrypted form on a Keno System. The encryption must meet cryptographic standards equivalent to the standards set out for encryption in the Australian Government Information Security Manual (ISM)¹².
- 7.4.9 The following information must only be stored using an encryption algorithm that adheres to the highest requirements defined in the Australian Government Information Security Manual (ISM) or Payment Card Industry Data Security Standard (PCI-DSS) standard or equivalent standard.
- i. Financial Institution PINs; or passwords and
 - ii. PINs or passwords used by players to access financial details of Keno System player accounts.

7.5 Player Account Statements

- 7.5.1 A Player Account statement must be available to the account holder upon request.
- 7.5.2 Player 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 Player Account statements must also include details of major wins.

7.6 De-activated and Dormant Player Accounts

¹² <https://www.asd.gov.au/infosec/ism/>

- 7.6.1 Any funds left in a Player Account which is to be de-activated are to be remitted to the owner of the Player 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 to securely identify and manage dormant or inactive players' accounts, including the treatment of unclaimed funds subject to 4.6.6 - 4.6.9 of this document.

7.7 Player Loyalty

- 7.7.1 The requirements of this section only apply if player loyalty is supported by a 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.
- 7.7.3 Use of player tracking data in development, testing and production environments must not breach the "Information Privacy Principles" referred to in section 7.3.3.
- 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 a 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 at Keno Venues

8.2.1 This section refers to requirements relating to the use of Keno Terminals at Keno Venues 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 a 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 adding credit to the SST via banknote, coin or financial institution 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 by Player Account holders

- 8.3.1 This section refers to requirements relating to Player Account holders placing Entries in a Keno game(s) via devices operating application software connected to online distribution methods.
- 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 Player Account balance after the transaction must be displayed to the customer on the input device, (e.g. screen) in currency value (dollars and cents).
- 8.3.5 Application software that enables holders of a Player Account to purchase entries to a Keno game must:

- a) Make available a display of the result of every game in which the player participates for a reasonable period of time;
- b) provide a means for an account holder to view past game entries and results, and, if applicable to that account holder, to view future game entries;
- c) display information about the game result in sufficient detail for the player to determine whether they have won or lost and the value of any winnings; and

8.3.6 It must be possible for the Player Account holder 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 A means of cancelling Account Entries must be provided to the extent practicable.

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

8.4.3 In the event that a 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.

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

8.4.5 Subject to the restrictions of section 4.8.6 and 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, a 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 .

without undue delay in either case following the validation of the win.

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 VGCCC 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 VGCCC 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 components of a Keno System via an approved communication medium with logical and/or physical security (e.g. serial data communications, if used, should be fitted with destructible seals and disconnection must be detectable), as required by the VGCCC.
- 9.1.4 VGCCC 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 unit must comply with section 4.1.4 and 4.1.5 of this document.
- 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 Destructible seals used to secure the RNG must be serialised.
- 9.1.11 The Licensee must establish processes and controls to record and audit RNG destructible seals.
- 9.1.12 The cage, case or cabinet must be shut, locked, and destructible seals fitted immediately after authorised works have been carried out.
- 9.1.13 The Licensee must notify VGCCC when the RNG cage, case or cabinet is accessed. The Licensee must ensure that keys to unlock the cage, case or cabinet must be secured and controlled.
- 9.1.14 The Licensee must notify VGCCC when the RNG cage, case or cabinet is accessed.

Logically Separate RNG

- 9.1.15 If the RNG is to be logically separated from a Keno System software, its software must be totally independent of the rest of a Keno System software.
- 9.1.16 All inner workings of the RNG must not be accessible by any of the other software.
- 9.1.17 Communication with a Keno System software must be only through controlled means in the same manner as if it were a physical connection.
- 9.1.18 Approval for the logical security of the RNG must be obtained from the VGCCC.

RNG Software Storage

- 9.1.19 VGCCC 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.
- 9.1.20 Prior approval must be obtained from the VGCCC each time the RNG program is to be changed.

Duplicated RNG Units

- 9.1.21 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 a Keno System computer systems there must be logically separated software in (at least) the back-up computer system(s).
- 9.1.22 The VGCCC does not require random selection of a RNG device.
- 9.1.23 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

- 9.1.24 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.
- 9.1.25 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.
- 9.1.26 The Licensee must establish strict controls and processes for any manual entries of Keno results.
- 9.1.27 The recorded output should show at least:
- i. Date;
 - ii. Time;
 - iii. A Keno Game number;
 - iv. The numbers drawn;
 - v. A unique checksum (that is to be entered with the numbers and checked by a Keno System when manual entry of numbers is required); and
 - vi. Other security information if available.
- 9.1.28 The recorded output must be held and be able to be accessed or retrieved for a minimum of seven years.

Record of RNG Logs

- 9.1.29 The RNG must have audit trails for logical accesses or tampering.

9.2 Communication with a Central System

Method of Communication

9.2.1 VGCCC approval must be obtained for the methods of communication from the RNG to the central components of a 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 components of a Keno System computer is to be secure and tamper proof.

Security of Connection of RNG Device

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

9.2.4 The Keno System must not allow commencement of a new game play when RNG is disconnected from the host.

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

9.3 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 VGCCC 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 the following must be included in submission-

- Provide full details in technical terms of random number and number selection/mapping.
- List all text and journal references where applicable used in the design of the RNG. Provision of this information may assist in reducing testing costs and the evaluation time.
- List all points in game play and the gaming program operation where the RNG is activated, updated, or numbers are obtained, including details of background RNG activity.
- Explain the seeding process of the RNG.
- Provide a detailed flow chart and software listing of the RNG process.
- Provide results for any empirical and/or theoretical tests conducted on the RNG.

9.4 RNG Test Modes

9.4.1 Simulator or 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 VGCCC 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 VGCCC 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 a 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 a 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 a 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 a 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 VGCCC and / or Tester in an approved machine readable form. Program and functional documentation should also be provided.

Separate Compilation Required

- 9.8.2 The VGCCC 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 a Keno System operator of possible non-random performance.