WAGERING AND BETTING SYSTEM REQUIREMENTS DOCUMENT

April 2012

Victorian Commission for Gambling and Liquor Regulation

State Government Victoria

Table of Contents

1 Glossary

This chapter sets out the glossary of standard terms and abbreviations relevant to the Wagering and Betting System Requirements document

Term or Abbreviation	Description
Account Betting	Bets placed against an account that has had monies deposited into the account before wagering or betting transactions can take place.
Act	The Gambling Regulation Act 2003 (Vic), as amended from time to time.
Agreement	Any related agreement entered into between the Minister and the Licensee in accordance with section 4.3A.10 of the Act.
Approved Betting Competition	Has the meaning given to that term in section 1.3(1) of the Act.
Approved Betting Contingencies	An approved betting product like a 'win' bet on which there may be an Approved Betting Competition.
Approved Betting Event	An event or class of event approved by the Commission under section 4.5.6 of the Act for betting purposes and includes a Sports Betting Event.
Approved Event	Collectively, an Approved Racing Event and an Approved Betting Event.
Approved Racing Event	An event or contingency, or a class of event or contingency, of or relating to a horse race, harness race or greyhound race approved by the Minister under section 4.5.3 of the Act.
Arrangements with VicRacing and Racing Products	The arrangements between the Wagering and Betting Licensee and VicRacing and the Licensee and Racing Products described in section 4.3A.7(2) (c) of the Act.
Baseline	A snapshot of an evolving system. The baseline also defines an envelope around a system (defined by the Commission) of which the Commission maintains verification control over. For example application files within a baseline would need approval prior to being modified, and there must be a method in place to verify baseline files have not changed since the last approval).

Term or Abbreviation	Description
Betting Rules	The betting rules for each bet type for the associated Wagering and Betting activity. Only approved betting, which may include fixed odds and pari-mutuel, may be conducted and must be in accordance with the Act.
Betting Exchange	A form of bookmaking which matches wagers between account holders, effectively acting like a stock exchange, for a Commission.
Card Security Value (CSV)	An additional security measure, usually a three or four digit number, printed on all credit cards that is unique to each card and only appears on the physical card; the CSV number cannot be obtained from statements or receipts.
Cash Exchange Mode	A betting option where an agent or device of the Licensee accepts wagers that are placed against monies, cash or debit card, received from the customer.
Collation	A record that contains an investment summary of all important selections for a pool. It may be a simple collation, such as a win pool, where the collation contains the investments on each selection in the event and a grand total. Or it may be a win type collation for a complex pool, such as a quadrella, where the collation contains the investments on the winning outcome(s) and the grand total.
Commission	The Victorian Commission for Gambling and Liquor Regulation or any of its successor organisations.
Commission's standards	The Commission's Gaming Machine standards, some aspects of which apply to the WBS. These consist of the Australian/New Zealand Gaming Machine National Standard and the Victorian Appendix to the Australian/New Zealand Gaming Machine National Standard.
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.
Cyclic Redundancy Check (CRC)	A non-secure hash function designed to detect accidental changes to raw computer data.
DMZ	A computer or small sub network that sits between a trusted internal network, such as a corporate private LAN, and an un-trusted external network, such as the public Internet. Typically, the DMZ contains devices accessible to Internet traffic.

Term or Abbreviation	Description
Firewall	A system or network component designed to block unauthorized access while permitting authorized communications; a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria.
Fixed Odds Betting	Offering each player specific odds, at the time of bet, that cannot vary in response to the subsequent betting activity and event information, except in some rare circumstances.
Fractional Betting	A bet where the amount of the investment on each combination covered by the bet is a percentage of the unit of Investment.
FTP	File Transfer Protocol - a method of transferring/exchanging files between computers over the internet.
Gaming Machine	Has the same meaning as defined in the Act.
Hardware	All physical components (electrical and mechanical) making up WBS Equipment.
Host	In the context of this document, a host is a physical or actual computer device, which may include both hardware and software. The WBS may include a number of hosts.
ICT	Information Communications Technology.
In-Running Betting	Betting while the event to which the bet relates is actually taking place; for example, placing a bet on a horse race while the race is being run.
Licence	The licence to conduct Wagering and Approved Betting Competitions as described in section 4.3A.1 of the Act.
Licensee	The holder of the Wagering and Betting Licence.
Minister	The Minister for Gaming for the State.
Memory	An area of a computing device used to store data and/or instructions.
Natural Person	A human being perceptible through the senses and subject to physical laws, as opposed to an artificial, legal or juristic person,
Pari-mutuel	Wagering or betting which involves player outlays being pooled, with a fixed percentage returned to players by the Wagering and Betting Licensee. Pari-mutuel Wagering or betting is run by means of a Totalisator.

Term or Abbreviation	Description
Parlay	A Wager in respect of which any resultant Dividend or Refund shall be re-invested in a subsequent event/pool.
Participating Outlets	Central locations, racecourses, hotels, clubs and retail wagering outlets in Victoria that use WBS Equipment for Wagering and Betting.
Plug and Play	A technique by which new hardware may be added to an existing computer and be automatically detected and configured.
Primary Site	The computer room(s) in which the WBS host(s) and related equipment are located.
QA	Quality Assurance - the methods an organisation puts in place to ensure reliable quality control.
Racing Products	Racing Products Victoria Pty Ltd (ACN 064 067 867).
RAM	Random Access Memory - the storage facility used by the CPU to store data and instructions. This form of storage is volatile: if the machine in which it is installed loses power, the contents of RAM are lost.
Regulation	A regulation is a form of secondary legislation issued by a government minister under the authority of primary legislation. Regulations are used to specify detailed arrangements by which the intent and purpose of primary legislation is to be carried out.
Regulator	The Commission or any of its successor organisations.
Reinstatement	The reversal of an earlier withdrawn selection from an event.
Responsible Gambling Code of Conduct	The Responsible Gambling Code of Conduct required under section 4.3A.5(2)(ab) of the Act and which may be amended from time to time.
Revision Number	A term used in Configuration Management. A revision number defines a baseline configuration of a system.
Rules	Refer to Betting Rules.
Scratching	A withdrawn selection from an event. There is a difference between Scratchings before the Official Scratchings, sometimes called Early Scratchings, and those after which are sometimes called Late Scratchings as the former can lead to the reduction in the number of Place dividends, or removal of a Place pool if the number of selections drops below a minimum, whereas the latter does not.

Term or Abbreviation	Description
Significant Event	Means the events set out in Sub-regulation Number 54 of the Gambling Regulation Regulations 2005.
Simulated Racing Event	Has the meaning given to that term in section 4.5.1 of the Act.
Sports Betting Event	An event, class of event or part of a class of event which is an Approved Betting Event designated by the Commission under section 4.5.9 of the Act as a Sports Betting Event.
Start Pay	A system related authorisation and command, once an event result has been entered and dividends calculated, that allows commencement of the payout process for an event.
Stop Pay	A system related authorisation and command to disallow or stop the payout process for an event.
State	The Crown in right of the State of Victoria and a reference to the State includes a reference to its servants, officers, agents and for the avoidance of doubt includes a reference to the Minister and the Secretary as the context requires.
Tester	A tester listed on the Roll of Manufacturers, Suppliers and Testers as defined in the Act.
Totalisator	A scheme of Pari-mutuel wagering, whether conducted by means of an instrument or contrivance known as a totalisator or otherwise, and the computerised system which runs Pari-mutuel wagering, calculating payoff odds, displaying them, and producing records based on incoming bets.
UPS	Uninterruptible Power Supply (a no-break mains power supply including battery backup equipment).
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 “version number”, "revision number", "revision level", or simply "revision".
Victorian Racing Industry	A collective term for the activities of horse racing, harness racing and greyhound racing in or in relation to Victoria and includes the regulation of such activities (whether mandatory or voluntary) and all stakeholders and participants thereof, including Racing Victoria, Harness Racing Victoria and Greyhound Racing Victoria.

VicRacing	VicRacing Pty Ltd (ACN 064 067 849) which is the entity responsible for administering the Joint Venture Arrangements between the Wagering and Betting Licensee and the Victorian Racing Industry.
Wagering	Pari-mutuel wagering on a horse race, harness race or greyhound race.
Wagering and Betting Business	The business of conducting Wagering and Approved Betting Competitions and the activities permitted by the Act on the Wagering and Betting Licence and related Agreement(s).
WBS	The Wagering and Betting System.
WBS Equipment	All of the instruments, contrivances or computer hardware, communications network or software that make up the WBS.

2
Foreword

This chapter introduces the background to the Wagering and Betting System Requirements document.

2.1 Wagering and Betting System

2.1.1 In April 2008, the government announced a new direction for Victoria's gambling industry. Under the new arrangements:

- The Wagering and Betting licence post 2012 is to be a single, exclusive Pari-mutuel and fixed odds licence.
- The Victorian racing industry will be funded from wagering operations post 2012 to the greatest extent possible.

2.1.2 On 3 November 2008, the government announced the proposed new tax arrangements that will apply to the Wagering and Betting Licence post 2012. The post 2012 Licence seeks to provide the Licensee with the flexibility to develop and distribute its products in response to the diverse needs and preferences of its customer base.

2.1.3 Subject to the Wagering and Betting Licence, the conditions imposed under section 4.3A.9 of the Act and the terms and conditions of any Related Agreement(s), the Licensee will be:

- Authorised to operate Wagering and Betting services (including the only authority to conduct Wagering and Betting via a Victorian retail network);
- Authorised to accept bets on a particular class of events using Approved Betting Contingencies for an event;
- Authorised to establish and operate a Betting Exchange in Victoria, to support account based betting;
- Authorised to conduct Approved Simulated Racing Events; and
- Required to enter into arrangements with Racing Victoria and Racing Products and Sports Controlling Bodies with respect to the use of their event content for Wagering and Betting purposes.

2.1.4 Subject to the approval of the Treasurer, State of Victoria, and the Commission, the Licensee will be able to enter into agreements to co-pool with other Pari-mutuel Wagering operators in Australia and Internationally.

3 Introduction

This chapter introduces the context and the purpose of the Wagering and Betting System Requirements document.

3.1 General Information

3.1.1 This Wagering and Betting System (WBS) Requirements document contains the related technical system requirements for Wagering and Betting Systems operating in Victoria.

3.1.2 All references in this document pertaining to the Licensee refer to the entity licensed to conduct the Wagering and Betting activity identified by its licence.

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

3.1.4 This document will be used by the Victorian Commission for Gambling Regulation (Commission) to evaluate compliance by the Licensee with the Wagering and Betting Licence and related Agreement(s), and to evaluate changes to a previously approved WBS, in accordance with 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 Agreement conditions, the Act and/or associated Licence and Agreement conditions will prevail.

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

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

Effective Date

3.1.7 These requirements and standards, as determined from time to time by the Commission, apply to the Licensee to operate a Wagering and Betting business from the Licence Commencement Date.

The Act

3.1.8 The requirements specified in this document are supplementary to and do not take the place of any of the requirements of the Gambling Regulation Act 2003 (referred to as 'the Act') or associated Licence and Agreement conditions (if any).

3.1.9 In approving the WBS or changes to an approved system, the Commission may take into account the certificate of a Tester under the section of the legislation applicable to the Wagering and Betting activities.

Objectives

3.1.10 The Commission sets high systems integrity standards for Wagering and Betting equipment operating in Victoria for the purpose of ensuring that:

i) The system operates in accordance with the Wagering and Betting Licence and related Agreement(s);

ii) The system operates in accordance with the Rules for the associated Wagering and Betting activity;

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

iv) All parties receive their correct entitlement.

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

Document Scope

3.1.12 The requirements in this document apply to WBS Equipment and systems to be operated by the Licensee according to the Wagering and Betting Licence and related Agreement(s) at central locations, racecourses and participating outlets in Victoria.

3.2 General Principles

3.2.1 The WBS must fully implement the Wagering and Betting Rules as supplied to the Commission by the Wagering and Betting Licensee.

3.2.2 The WBS must implement the Betting Rules for the calculation of dividends, payouts, reinvestments and jackpots. The factors that may need to be addressed by the Rules and the WBS include, but are not limited to:

i) commissions;

ii) Dividend formulae;

iii) Withdrawn selections;

iv) Multiple winners of a bet type;

v) Abandoned events, including but not limited to:

   a) Refunds of wagers;

   b) Field payouts, where dictated by the Rules;

vi) Re-run events, including but not limited to:

   a) WBS handling and procedures for the circumstance where a re-investment cannot be processed, e.g. because results of a re-run event are not finalised, and a subsequent event that would have had re-investments added to its collation is run; and

   b) WBS handling and procedures for the circumstance and treatment of winners where the re-run event is part of a multi-leg pool;

vii) No winners of a pool or a component of a pool, including but not limited to:

a) Count-back levels; and

b) Jackpots;

viii) Rounding calculations for dividends, payouts, reinvestments and jackpots;

ix) Jackpot amounts transferred in or out of a pool; and

x) Minimum prize payouts.

3.2.3 A Start Pay must only be permitted by the WBS in accordance with the Betting Rules.

3.2.4 The WBS must implement the Betting Rules for dealing with a withdrawn selection. The Betting Rules and the WBS should address but not be limited to the following:

i) Circumstances when all bets on a selection are lost when the selection is withdrawn, e.g. 'all-in' betting;

ii) Circumstances when all bets on a selection are refunded when the selection is withdrawn;

iii) Handling of withdrawn selections for bets involving multiple events, e.g. parlays;

iv) Handling of reinstated selections;

v) Reduction in the number of dividends for a pool or removal of a pool, e.g. a place pool. If a scratching reduces the field size below a certain threshold, the WBS must be able to distinguish between a scratching before the official scratchings are determined, sometimes called early scratchings, and those after the official scratchings, which are sometimes called late scratchings.

vi) If appropriate, the calculation for a substitute where one is required to replace withdrawn selections such as in multi leg pools, e.g. Doubles; and

vii) If appropriate, the handling of the situation where one or more selections in a bracketed selection are withdrawn, including all of the selections in the bracket;

3.2.5 The WBS must provide a user friendly facility to allow a player the ability to attempt to cancel any active bets.

3.2.6 The WBS must provide a player with access to the Betting Rules, including but not limited to the Rules relevant to the prevention of cancellations.

3.2.7 If the Betting Rules cater for circumstances where rounding can occur, for example parlay re-investments or fractional betting, the WBS must implement correct handling and accounting of any rounding that may occur.

3.2.8 The WBS must implement all aspects of account based betting in accordance with the Betting Rules. Refer to section 7 for Player Account requirements.

3.2.9 Account based wagers may be placed through the WBS but only after a log-in to an existing account with appropriate security control e.g. PIN.

3.2.10 The WBS must enable changes to the WBS in a timely manner to reflect changes in the Betting Rules, e.g. a change of pool commission. The method(s) and mechanism(s) enabling such changes must be able to be tested by a Tester in accordance with the testing requirements in section 13 and the submission requirements in section 14 of this document.

3.3 ICT Service Management Framework

3.3.1 In order to ensure that the WBS and its associated equipment operate as approved by the Commission, the Licensee must establish and maintain policies, standards and procedures that the Licensee will use to develop, implement and operate a WBS, including but not limited to:

i) Service desk, incorporating the Help Desk;
ii) Incident management;
iii) Problem management;
iv) Change management;
v) Release management;
vi) Configuration management;
vii) Application management;
viii) Availability management;
ix) Capacity management;
x) Service level management;
xi) Financial management;
xii) Service continuity management;
xiii) Security management; and
xiv) ICT infrastructure management.

3.4 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 Commission.

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

System Performance Standards

3.4.3 The WBS must be capable of meeting the performance standards set out in the Wagering and Betting Licence and related Agreement(s).

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

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

3.4.6 The WBS must be capable at all times of determining whether all Components of the WBS that operate software or firmware in connection with the Wagering and Betting Business are functioning.

Responsibilities

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

3.5 Approved WBS Equipment

Approval of WBS Equipment

3.5.1 Only approved WBS Equipment may be operated in Victoria.

3.5.2 Approval must be obtained from the Commission before any equipment capable of affecting the integrity and conduct of Wagering and Betting activities, as determined by the Commission, becomes part of the WBS.

3.6 Commission Standards for Gaming Machines

3.6.1 Some requirements in this standard are common to Gaming Machines and hence may refer to the Commission Standards regarding Gaming Machines.

3.6.2 The Australian/New Zealand Gaming Machine National Standard and the Victorian Appendix to the Australian/New Zealand Gaming Machine National Standard defines the Commission Standards for Gaming Machines.

4
Wagering and Betting System

This chapter sets out the WBS requirements that must be followed for the Wagering and Betting Licensee's operation in Victoria.

4.1 WBS Environment

4.1.1 The Commission requires the Licensee to implement the computerised WBS capable of meeting the following broad functions:

i) Efficiently perform all tasks associated with operating a Wagering and Betting system;

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

iii) Comply with the applicable Betting 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 Commission.

4.1.2 A computerised WBS is deemed to extend to the point at which:

i) A customer's gambling transaction is presented; or

ii) System generated gambling information is delivered to/from the WBS interface in an approved format.

4.1.3 The WBS shall be designed in consideration of the following usability principles:

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

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

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

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

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

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

vii) Flexibility and efficiency of use through design that caters to both inexperienced and experienced.

viii) Aesthetic and minimalist design ensuring relevant and necessary information is prominently displayed.

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

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

4.1.4 The WBS shall be designed in consideration of the Whole of Victorian Government ICT Standard for Accessibility, available from the eGovernment Resource Centre, maintained by the eServices Unit, Information Victoria - a unit within the Department of Innovation, Industry and Regional Development (DIIRD).

Electromagnetic Interference

4.1.5 When subjected to human body or any other source of electrostatic discharges, a WBS component must not severely interfere with any other connected WBS component.

4.2 WBS Primary Site Accommodation

Physical Security

4.2.1 The WBS datacenters must be a secure area where only authorised personnel can enter. The Commission requires the adoption of an electronic locking system that provides monitoring information on the entry and exit of all personnel.

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

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

4.2.4 The Licensee must ensure that an accredited external and independent Security Testing company undertakes testing of the physical security of the computer room(s) and related WBS Equipment every six months and provide a written report of its findings. This report must be provided to the Commission within two weeks of its receipt and must include details of action(s) taken, and planned actions, by the Licensee with respect to all issues identified in the report.

Environmental Monitoring System

4.2.5 All WBS Equipment within the computer room(s) environment must be supported by an environmental monitoring system that will perform automated switching to backup systems for most component failures of the environmental 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 the equipment and to automatically alert if these conditions are not met.

Power Supply

4.2.7 All WBS Equipment and powered devices within or contributing to the 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 a WBS component is disrupted, the component must not severely interfere with the operation of any other WBS Equipment, including equipment external to the WBS computer room(s).

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 Wagering and Betting business, must be tested at least every three months. These reports will only be required by the Commission when the Commission 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 Commission, and the Commission 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 WBS and within the reasonable control of the Licensee 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 WBS datacenters on full load until a stand-by generator(s) is started. In the event that the generator(s) are unable to start, it must enable the systems to be shut down in an orderly manner without the loss of data.

4.2.14 All equipment situated in the computer room must be earthed via the UPS.

Stand-by Generator

4.2.15 The primary site and related WBS Equipment 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 WBS Equipment and facilities for a period of not less than 24 hours.

Emergency Lighting

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

Help Desk System

4.2.17 A “Help Desk” facility must be provided to assist customers and participating outlets and personnel with problems, disputes and maintenance calls and be available whenever Wagering and Betting is scheduled through any medium.

4.2.18 The Help Desk operators are to have secure on-line access to the WBS to enable them to perform these activities.

4.2.19 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 outlets and personnel to establish contact with Help Desk operators during critical events without unreasonable delay.

4.2.20 All calls to the Help Desk must be logged and the log made available to the Commission 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) Caller identifier and contact details where required for audit and or follow up actions;

iii) The issue prompting the call; and

iv) Details of the outcome of the call.

4.3 WBS Host

4.3.1 The WBS must operate in accordance with the rules and regulations associated with operating a Wagering and Betting business as consented to by the Commission.

4.3.2 Commission approval must be obtained for the software and hardware configuration (baseline) of the WBS host and related WBS Equipment.

System Baseline Document

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

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

4.3.5 Commission approval must be obtained by the Licensee for the baseline document, including any changes to the baseline document.

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

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

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

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

i) All the system components which represent the core components of the WBS for operating a Wagering and Betting Business including but not limited to any WBS host and any WBS Equipment including equipment located in participating outlets;

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

iii) Hardware platforms;

iv) Operating systems;

v) Interface modules that interact with databases used by the system application;

vi) Interface devices and related software that interacts with any neighbouring application, external system, remote outlet or third party services;

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

viii) The method and mechanisms used to verify that the system is operating in an approved configuration;

ix) A Network Policy Document, in accordance with the requirements in section 5.3, Network Requirements, which clearly identifies the core areas of the WBS network including but not limited to the network topology of the system, detailing the interconnection of modules within the network, the type of connection between the modules, and the communication protocols that are permitted;

x) Identification of any operations or procedures relevant to securing control of the system; and

xi) Identification of any other special operational or procedural issue that is relevant to the Commission.

4.3.10 A Tester's recommendation must be obtained by the Licensee for all changes to the System Baseline Document, including any emergency changes.

4.3.11 Commission approval must be obtained by the Licensee for any changes to the baseline document, including any emergency changes, having regard to any relevant Tester's recommendation.

4.3.12 The baseline document must specify the location of application files and configuration files.

4.3.13 The WBS must have a method to verify the baseline system application executable files (and selected command utilities) in order to confirm that the configuration of the system is operating in an approved state.

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

4.4 WBS Software Procedures

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

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

4.4.3 Only an approved configuration may reside on storage devices or in the memory of the WBS computers. The approved configuration may incorporate the existence of and/or the contents of any of the following items:

i) Operating system files (including supporting files such as patches, service packs, device drivers and configuration files);

ii) Application executable files (including supporting files such as configuration files and selected command utilities); and

iii) Temporary working and log files.

WBS Software Quality

4.4.4 Refer to sections 6.6 and 6.7 of this document.

4.5 Logging of Information

4.5.1 Data relating to financial accounting, Wagering and Betting activity statistics, Significant Events, security logs and WBS configuration data must be held in a (backed-up) computer system.

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

4.5.3 All accounting and any Significant 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.

4.6 Retention of Unclaimed Monies and Dormant Accounts

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

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

4.6.3 The Licensee must hold money that has not been claimed, or money related to dormant accounts, in trust for distribution as required by relevant legislation.

4.6.4 The serial numbers (refer to section 9.2.11) or other access method for "old" unclaimed monies stored on the system (e.g. unclaimed payout/prize tickets), must be secured, and the method used to secure the information must ensure that a program cannot be run to provide a list of unclaimed monies that might be obtained and/or used without authorisation.

4.7 Program Storage Devices

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

4.7.2 Any WBS device 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.

4.8 Significant Events

4.8.1 The Licensee must establish and maintain policies, procedures and standards for reporting Significant Events to the Commission.

4.8.2 On discovering a Significant Event in respect of a totalisator or an approved betting competition conducted by the Licensee, the Licensee must, without delay and not more than 24 hours after the discovery, report the occurrence of the Significant Event to the Commission and provide to the Commission any further information in relation to the occurrence of the Significant Event that the Commission may require.

4.8.3 The sub-regulation[1] defines Significant Events as:

i) An error in the calculation of a dividend or prize;

ii) An error in the calculation of the money available for dividends;

iii) The acceptance by the operator of a bet:

a) In the case of a bet in a totalisator – after the start of the event on which the bet is accepted; or

b) In the case of a bet in an approved betting competition – after the start of the event in respect of which the bet is accepted or after the operator has indicated that it is not accepting, or has ceased to accept, bets in respect of that event, whichever is the later;

iv) The manipulation or attempted manipulation by a person employed by the operator of the equipment (including computer software) used in connection with wagering or approved betting competitions;

v) The misuse by a person employed by the operator of information obtained by that person as a result of his or her employment;

vi) The presentation of a forged ticket or the forgery or attempted forgery of a ticket in respect of a totalisator or an approved betting competition;

vii) The cancellation of a bet after the result of the event on which the bet was made has been decided;

[1] Sub-regulation Number 54 of the Gambling Regulation Regulations 2005

viii) A period of time in excess of 10 minutes during which the operator is unable to accept bets when the operator's betting offices are open for business; and

ix) The activation of the operator's emergency procedures or disaster recovery procedures in connection with the operator's totalisator business.

4.8.4 In addition, the Licensee must be able to record and report, as required by the Commission, the following other events:

i) Circumstances where the system is incapable of supporting the Betting Rules;

ii) System failures;

iii) Instances where there has been any form of unauthorised access to any component of the WBS or related accommodation and facilities;

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 WBS 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) Other instances where late closures were identified;

x) Other instances where incorrect payouts/prizes were identified;

xi) Other payments in excess of designated monetary values; and

xii) Abnormal changes in an event or race day schedule including but not limited to:

a) Modification of an event results;

b) Reopened events/pools; and

c) Change of commission for any pool.

Generation of Significant Events

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

Storage of Significant Events

4.8.6 The Significant Events prescribed by the Gambling Regulation Regulations 2005 and the other events listed in 4.8.4, regardless of the source of these events, are to be stored at the Licensee's premises.

4.8.7 All Significant Events must be stored electronically in a manner approved by the Commission.

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

4.8.9 Significant Events must be detected and recorded within a timeframe approved by the Commission, which may vary depending on the source of the Significant Event. If the source of the Significant Event can be detected electronically then the Significant Event must be detected and recorded within 10 seconds of the occurrence of the Significant Event.

4.8.10 Significant Events must be reported within 10 seconds of the recording of the Significant Event.

Recovery of Significant Events

4.8.11 In the event of the failure of the WBS host it must be possible to electronically recover the Significant Events using a method that ensures no Significant Events are lost.

4.9 WBS Security

4.9.1 The Licensee must establish and maintain policies, procedures, standards and mechanisms for adequate security over the approved system, including but not limited to virus prevention, detection and correction, 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 for any access to any configuration item or function of the system, including but not limited to system users, system operators, system developers and system administrators.

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

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

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

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

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

v) Procedures for adequate protection of emergency passwords.

4.9.4 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 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 Variations on the process and procedures for securing programs and data files under 4.9.6 may be approved by the Commission.

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

4.9.9 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 Commission.

4.9.10 The Licensee must ensure that access to specific functions within the WBS 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) Configuration and administration of system parameters regarding:

a) Approved Betting Competitions;

b) Approved Betting Contingencies; or

c) Approved Betting Events;

ii) Configuration and administration of Betting Rules;

iii) Any other system parameter changes;

iv) Installation of new versions of software; and

v) Other functions as determined by the Commission.

4.9.11 The Licensee must develop and maintain policies and operating procedures designed to prevent hacking or unauthorised access to the WBS and WBS Equipment.

4.9.12 The Licensee must ensure that an accredited external and independent Information Technology IT Network and Security Testing company undertakes system and network vulnerability penetration testing on its WBS and WBS Equipment every six months and provide a written report of its findings. This report must be provided to the Commission within two weeks of its receipt and must include details of action(s) taken, and planned actions, by the Licensee with respect to all issues identified in the report.

System Audit

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

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

ii) Critical issues management;

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

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

v) Software integrity;

vi) Peripheral equipment integrity;

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

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

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

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

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

xii) Software change control aligned with change management processes; and

xiii) Emergency change control.

4.9.14 The Licensee must establish and maintain policies, procedures and standards for the use of data editors, utilities or related software such as SQL, for database access or update (manual or otherwise). In any case, these must not be accessible by unauthorised persons.

Access by Commission

4.9.15 The Licensee, at the direction of the Commission or an Inspector appointed under section 10.5 of the Gambling Regulation Act 2003, must provide online, read only access to the information on the WBS application and database at any time.

4.9.16 The Licensee must provide tools and mechanisms to:

i) Examine Significant Events;

ii) Examine data; and

iii) Verify the approved system baseline.

4.9.17 The communication link between the Commission and the Licensee must be encrypted and meet the minimum standard identified in section 5.1 of this document.

4.10 WBS Recovery

4.10.1 The Licensee must have policies, procedures and standards in place in accordance with Commission guidelines for WBS data and software recovery and any relevant component of it.

Transaction Logging

4.10.2 A complete log of transactions since the last backup is to be maintained at a disaster recovery site approved by the Commission. The disaster recovery site should meet the standards required for the primary site as set out in this document.

4.10.3 For transaction logging the Licensee must ensure that:

i) The WBS must record in a log file(s) or database with time and date stamp all vital transactions (as defined hereafter in paragraphs 4.10.15 - 4.10.17) received from any equipment that processes a wagering or betting transaction;

ii) The log file(s) and/or database must be duplicated for reliability. Mirrored disk copies are not considered sufficient for the duplication requirement unless they are application software generated;

iii) Commission approval must be obtained for the method of transaction logging;

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

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

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

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 that is approved by the Commission, and the following minimum information is to be included with each log record:

i) The date that the transaction/event occurred;

ii) The time that the transaction/event occurred;

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

iv) Any relevant data that is associated with the event; and

v) A unique event identifier which defines the transaction/event.

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

Disaster Recovery and Business Continuity

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

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

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

4.10.11 The Licensee must establish and maintain a disaster recovery test plan, including a schedule for testing, and conduct disaster recovery testing in accordance with the plan. The plan and test schedule must be submitted to the Commission.

4.10.12 In the event of a disaster, there must be a method of ensuring that all data and information related to WBS Equipment, WBS transactions, customer entitlements and government revenue (since the last backup and the transaction log) can be rebuilt up to the point of the disaster.

4.10.13 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.

4.10.14 There must be periodic back-ups (at least daily) of the variable database files on the WBS's storage devices.

System Data Recovery

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

i) Significant Events;

ii) Cash tickets generated and/or cashed including current account balances;

iii) Account information including winnings, bets, cash deposits and cash withdrawals, PIN change, expiry date, site where issued, account closure;

iv) Manual database updates;

v) WBS network reconfiguration including but not limited to additions, deletions or modifications of WBS Equipment;

vi) WBS software reconfiguration including but not limited to WBS host or remote application(s) software versions, Betting Rules, configuration tables, or reference data;

vii) Betting transactions including source, meetings, pools, selections, wager amounts, odds (if a fixed odds wager), and status for each betting transaction in the system;

viii) Cancellation transactions including cancellation amount, relevant pool(s) and operator identification if a late cancel;

ix) Schedule entry/approval, including selection/participant names;

x) All race-day control commands, including but not limited to start/stop sell, start/stop pay, scratchings/reinstatements, results entry, meeting/race/pool abandons, and schedule alterations;

xi) All dividends calculated including winning selection(s), dividend amounts, fractions and subsidies;

xii) Input and output Jackpots and related Jackpot transactions including contributions, winnings and current value for each jackpot in the system;

xiii) Any adjustments to fixed odds payouts including the reason;

xiv) System parameters regarding:

a) Approved Betting Competitions;

b) Approved Betting Contingencies; or

c) Approved Betting Events;

xv) Current system encryption keys; and

xvi) Any other system parameters, modifications, reconfiguration (including participating outlets), additions, merges, deletions, transfers and display parameter changes.

4.10.16 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 approved by the Commission.

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

WBS Failure Modes and Recovery

4.10.18 Following any failure, it must be possible to restore the state of the WBS and its database(s) without losing data as defined in 4.10 WBS Recovery.

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

4.10.20 Some typical tests that may be implemented by the Commission or its representatives in a test environment to test compliance with this and other sections of the document are:

i) Failure of computer processor;

ii) Failure of computer power supply;

iii) Failure of computer memory;

iv) Failure of computer disk(s);

v) Failure of computer I/O channels;

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

vii) Total power failure of the WBS host or primary 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 stored data and the encryption used must meet cryptographic standards equivalent to the standards set out for encryption in the Australian Government Information and Communications Technology Security Manual (ISM)[2].

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

i) Personal Identification Numbers (PIN); and

ii) All forms of password.

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

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

i) Encryption/decryption keys; and

ii) Unclaimed tickets and critical fields such as serial numbers and authentication codes.

PIN and Password Management

4.11.4 If a customer's or WBS 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 by the Commission prior to approval.

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

4.12 WBS 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 Commission approval must be obtained for the configuration management plan and the configuration of a WBS.

4.12.3 The assessment will evaluate the configuration for operational integrity as well as reliability, recoverability, audit ability, redundancy and security.

Security of Event and Transaction Logs

4.12.4 The system must prevent the changing of the Significant Events log and/or significant Wagering and Betting transactions. It is mandatory that the event and transaction logs and software be structured so that it is not possible for there to be unauthorised modifications. This will involve both password security control and ensuring that the only valid method of writing to the event and transaction logs is sequential (i.e. no random update methods are to be permitted).

Multiple Data Files

4.12.5 There must be at least two electronic copies for each file and/or database that contains the vital information documented in section 4.9 WBS Security and section 4.10 WBS Recovery. For this requirement, mirrored disk files (which are a way of protecting against one form of failure) are not considered adequate for the criteria unless they are application software created.

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

Data and Event Monitoring

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

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

4.12.9 This facility is not required to be a component of the system baseline.

Documentation and Reporting

4.12.10 Details of the Commission's reporting requirements are to be provided to the Licensee by the Commission.

Commission Required Reports

4.12.11 Financial information reports, including taxation, by event conducted must be made available to the Commission in a format and of a frequency specified by the Commission that is compatible for processing by the Commission's systems.

4.12.12 Reports of any security breach or attempted security breach of the WBS, including but not limited to breaches or attempted breaches of a system firewall, must be made available to the Commission in a format and of a frequency specified by the Commission.

4.12.13 Reports supplied to the Commission must be complete, comprehensive, accurate, clearly delineated, be able to be clearly printed, and available in electronic format.

System Integration

4.12.14 The Commission may approve the integration of all sub-systems or utilities with the WBS and WBS Equipment in general, 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 Wagering and Betting business.

4.12.15 The real-time monitoring and inspection facility described in 4.12.7 of this document is not required to be a component of this approval process.

4.12.16 The integration of the WBS with sub-systems or utilities must be described in the configuration management plan.

Link to Commission Computing Facilities

4.12.17 The real-time monitoring and inspection facility described in 4.12.7 of this document must include a secure electronic link, equivalent to the standard identified in 4.11.1 of this document, from the Licensee's WBS primary site to the Commission's computer facilities.

4.12.18 The real-time monitoring and inspection facility may be used for down loading financial data and the reports described in 4.12.11 of this document on a daily basis (or at a frequency agreed by the Commission).

4.12.19 The data link between the Commission and the Licensee's WBS site must implement cryptographic data security as detailed in section 5.1 of this document.

4.12.20 The data link between the Commission 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

Facilities for Inspectors

4.12.21 Facilities for 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 prize configuration tables, where applicable;

iii) Ability to perform signature checks

iv) Ability to verify that Wagering and Betting terminals and other WBS Equipment are on-line;

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

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

vii) Provision for technical assistance to perform all the above;

viii) Ability to review financial data;

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

x) Provision of technical assistance on request from the Commission to assist inspector's in the conduct of technical compliance.

5 Network and Communications

This chapter sets out the WBS 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 single logic area;

ii) Cryptographic data security must apply for all critical data communication transfer between all WBS Equipment at a participating outlet, and between a participating outlet and the WBS host (but not necessarily within the primary 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 WBS algorithms and information related to government revenue;

g) Vital transactions related to the operation of a Wagering and Betting business; and

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

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

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

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

c) Transfer of money between gaming equipment.

Encryption Algorithm Approval

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

i) Encryption algorithms are to be demonstrably secure against cryptanalytic[3] attacks;

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

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

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

Message Authentication Algorithm Approval

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

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

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

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

Encryption Keys

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

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

5.2 Communications Requirements

Data Communications Protocol

5.2.1 Commission approval must be obtained in advance for any protocol used for data communications between WBS Equipment.

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

5.2.3 The Commission will only approve a protocol if it is confident that the devices implementing the protocol will fully comply with the requirements of this document and any other Victorian standards.

Data Communications Links

5.2.4 Communications protocols must include the following:

i) Error Control;

ii) Flow Control; and

iii) Link Control (remote connection).

Data Communication Error Detection

5.2.5 Communications protocols must make use of CRC's or the equivalent - use of only parity or simple checksum byte is not acceptable.

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

Communication Failure Modes and Recovery

5.2.7 All WBS Equipment must be recoverable to the point of failure following an interruption.

5.2.8 A Tester may test the communications infrastructure for resilience, recoverability and continuity of service, including but not limited to conditions for:

i) Failure of WBS LAN interfaces;

ii) Failure of LAN;

iii) Failure of data communication interface devices;

iv) Failure of a single data communication interface;

v) NTU failure at the primary site;

vi) NTU failure at a remote site;

vii) High data communications error rates on line;

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

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

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

xi) LAN failure on a regional or local controller (if any); and

xii) LAN failure on cashier terminal (if any).

5.3 Network Requirements

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

5.3.2 These network requirements apply equally to Participating Outlets and WBS networks.

Network Baseline

5.3.3 During the approval stage of a system network, and based on the System Baseline Document prepared by the Licensee, the Commission will determine the core areas of the system network that it will maintain verification control over and this will be defined and approved in a Network Policy Document. This document is the responsibility of the Licensee to prepare as part of its submission to the Commission when obtaining approval for the WBS. It is essentially a matrix that describes the network topology of the system, details the interconnection of modules within the network, and the type of connection between the modules that is permitted.

Physical Requirements

5.3.4 Power to devices inside and on the boundary of the baseline envelope must be provided from a filtered, dedicated power circuit. As a minimum standard, this requirement applies to any WBS Equipment that is capable of affecting the outcome of a Wagering and Betting transaction.

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

Network Documentation

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

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

Connection of External Devices to Networks within a Baseline Envelope

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

5.3.9 The facilities for plug and play installation of devices must be disabled.

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

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

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

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

Communications within a Baseline Envelope

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

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

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

5.3.17 All information traversing the network between remote equipment and the WBS host must be recoverable once communications are restored.

Communications between Separate Baseline Envelopes

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

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

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

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

5.3.22 Communication between devices in separate baseline envelopes will be protected and should 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)

5.3.23 Data exchanged with computer systems and terminals outside the baseline envelope must pass through at least one network control device (router or firewall). The network control devices must implement the controls as defined in the Network Policy Document, which must be prepared by the Licensee and submitted to the Commission for approval.

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

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

5.3.26 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.

5.3.27 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.).

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

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

i) Authentication scheme;

ii) Physical and logical security of the external terminal devices and computer systems;

iii) Physical and logical 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 WBS pertaining to the transfer (date, time, person account or system account, and file(s) transferred); and

viii) Intrusion detection utilised and immunity from computer attacks.

Note: WAN communication links will be generally deemed to be outside a baseline envelope.

Computer Monitoring Systems and Network Management Systems

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

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

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

5.3.33 A device outside a baseline envelope must not be able to affect the configuration of network devices or network control devices by any means, including but not limited to:

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

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

iii) Replaying previously captured communications.

5.3.34 A device outside a baseline envelope must not be able to affect the operation of the WBS or be able to read or modify critical data.

Internet Connections

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

5.3.36 The WBS, at the point where it is connected to the Internet service provider, must incorporate a DMZ-like architecture.

5.3.37 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.

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

Verification Tools

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

5.4 Wireless Communication

5.4.1 Wireless communication may be acceptable to the Commission provided that there are appropriate additional security measures in place, which meet the standards set out for wireless communication in the Australian Government Information and Communications Technology Security Manual (ISM)[4], to overcome the general weaknesses of wireless communication.

5.4.2 Wireless communication will be considered for Local Area Network communications and/or Wide Area Network communications.

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 network unless a stand-alone stateful packet inspection firewall is employed.

5.4.5 Wireless network traffic must be secured with additional encryption and/or authentication codes and must meet the requirement 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 Commission will consider performance and availability before granting approval to the use of wireless communication.

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

6
Wagering and Betting System Equipment

This chapter sets out the requirements for WBS Equipment that must be followed for operation in Victoria.

6.1 General

6.1.1 Approval must be obtained from the Commission before placing into service, any equipment, software or procedures which form an integral part of the approval.

6.1.2 It is the Licensee's responsibility to install and maintain all equipment that is a part of the WBS.

6.1.3 The WBS Equipment will provide the means for selling, paying, cancelling bets and other transactions associated with a Wagering and Betting business.

6.1.4 The WBS Equipment must enable Wagering and Betting transactions to be carried out in a manner that is auditable, reliable, secure and fair to customers.

6.1.5 All WBS Equipment functions relevant to the operation of a Wagering and Betting business must be approved by the Commission.

6.1.6 All WBS Equipment functions not relevant to the operation of a Wagering and Betting business must not interfere or affect any equipment functions that are pertinent to the operation of a Wagering and Betting business.

6.1.7 All WBS Equipment and its associated functions must be access protected and must not be capable of any function when a WBS operator is not logged on.

6.1.8 Commission approval must be obtained for the method and security of communications to and from any WBS Equipment.

6.2 Hardware Requirements

6.2.1 The design and configuration of all WBS Equipment hardware and any changes to WBS Equipment hardware must be submitted to the Commission for approval.

6.3 Maintenance Requirements

6.3.1 Maintenance of WBS Equipment that is the responsibility of the Licensee is only to be conducted by an organisation(s) that is listed on the Roll of Manufacturers, Suppliers and Testers and is contracted by the Licensee.

6.3.2 All scheduled maintenance should be carried out in accordance with a maintenance schedule that has been approved by the Commission.

Retention of Data

6.3.3 All equipment statistics, Wagering and Betting information and metering information stored in the equipment (whether by electronic, magnetic, mechanical or other means) shall be retained during hardware maintenance and shall be protected against damage, destruction or alteration during maintenance operations (including battery replacement).

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

Maintenance Not to Infringe Approval

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

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

6.3.7 Hardware maintenance of equipment shall not be by any of the following means:

i) Testing and fault diagnosis requiring the cutting of electronic circuitry;

ii) Testing and fault diagnosis requiring the drilling of electronic circuitry;

iii) Testing and fault diagnosis requiring the addition of electronic circuitry;

iv) Thermal overstressing of components; or

v) Removal or insertion of components while power is applied to the equipment, unless the equipment has been specifically designed to withstand such actions and then only by following the appropriate procedures laid down by the manufacturers.

6.3.8 All hardware maintenance will follow industry best-practice with respect to protecting the equipment from static discharge. In particular, where appropriate, the following shall be observed:

i) All components and assemblies must be stored and transported in anti-static packaging at all times;

ii) No components or assemblies are to be touched unless the technician is earthed via a wrist strap or other earthing device; and

iii) Maintenance work-areas must be earthed and fitted with earthed floor mats, earthed bench mats and wrist strap earth points.

6.4 Information Displays

6.4.1 Commission approval must be obtained for information that is to be displayed on WBS Equipment and the method of display of information. The guidelines for such approval will be Victorian Legislation and Regulations and accepted community standards.

6.4.2 Displays must communicate with controlling devices via a protocol based form of communication.

6.4.3 “External” Displays employed in communicating the results of events and games will be considered on a case-by-case basis by the Commission.

6.4.4 Video monitors, touch screens and printers used as information displays must meet the requirements set out in sections 2.4.33 to 2.4.39 of the Australian/New Zealand Gaming Machine National Standards.

6.5 Banknote Acceptance

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

6.6 Software Requirements

6.6.1 Commission approval must be obtained for the design and configuration of all WBS Equipment software and any changes to WBS Equipment software including but not limited to WBS Equipment for participating outlets.

6.6.2 All software must meet the Software Requirements set out in section 3 of the Australian/New Zealand Gaming Machine National Standard and section V3 of the Victorian Appendix to the Australian/New Zealand Gaming Machine National Standard.

6.7 Software Functionality

Source Software

6.7.1 The Licensee will provide (where possible) the source software for all WBS Equipment to the Commission and/or a Tester where it has access to such information in an approved machine readable form. Any program and functional documentation that the Licensee has access to may also be provided.

6.7.2 Source software supplied to the Commission, and/or a Tester, shall be exactly as installed, programmed or loaded in the equipment to be used.

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

i) Module name;

ii) Revision Level;

iii) Brief description of functions performed; and

iv) Edit history: who, why and when (of changes made after this date).

Source Compilation

6.7.4 The Commission requires the ability to verify that the WBS program(s) being compiled and deployed to the production environment are identical to the programs being evaluated.

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

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

6.7.7 The Licensee will provide (where possible) access to tools or proprietary development environments for to the Commission and/or a Tester where it has access to such.

Source Control and Upgrade

6.7.8 Separate approval must be obtained from the Commission for each software revision.

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

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

Software Functions Provided

6.7.11 All implemented functions must operate according to the intended design, all messages displayed must be true and accurate and reasonable care must be taken to ensure that the software is free from defects or errors.

Software Verification During Development

6.7.12 The Licensee, and/or suppliers of WBS software, must provide a method to the Commission to enable confidence to be gained that the software on which evaluation was performed, the software on which system testing was conducted and the software finally submitted for live operation are directly equivalent. To this end the following goals are to be met:

i) Source software will be provided to the Commission or a Tester in a machine readable form where the Licensee has the capability, right, or access to source to provide (which may be the IP of a third party provider);

ii) There must be a method available, to the Commission or its representatives, for examining the source software and conducting computer aided searches;

iii) There must be a method available, to the Commission or its representatives, for comparing two different versions of the source software and examining the differences between the two versions;

iv) There must be a method available of verification that the executable software that is to be used for testing has been compiled from the source software versions submitted to the Commission;

v) If software changes are required during the testing process, in accordance with the requirements at section 13, all changes must be submitted via the source software. Examination of differences and verification of executable or data files will be undertaken by the Commission or its representatives by compiling the submitted source software;

vi) There must be a method available to verify that the executable software that has been used during the testing process is identical to that which is to operate on the live system. This verification procedure must occur when new software is installed, at the start of each trading day by the Licensee and randomly on demand by the Commission; and

vii) There must be a method available to determine if unapproved programs, command files, fixed data files, etc. reside on any component in the WBS system.

6.7.13 Formal testing will not commence on any system if the first four steps in 6.7.12 are not in place. Live operation will not be approved until all steps are in place.

7
Player Account Requirements

This chapter sets out the requirements that must be followed for account based Wagering and Betting activities carried out in Victoria.

7.1 Player Accounts

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

7.1.2 The WBS must not accept a bet that would cause a player account to become negative.

7.2 Creation of Player Accounts

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

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

7.2.3 The Licensee must carry out a Proof of Identity check for each applicant. Full access to account functionality, including but not limited to the ability to withdraw funds from the account, cannot be granted until the Proof of Identity checks have been completed.

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

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

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

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

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

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

7.3 Privacy of Player Information

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

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

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

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

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

7.4 Player Accounts Maintenance

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

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

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

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

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

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

7.4.7 Personal information of a sensitive nature must only be stored in an encrypted form on the WBS. The encryption must meet cryptographic standards equivalent to the standards set out for encryption in the Australian Government Information and Communications Technology Security Manual (ISM)[5].

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

i) Financial Institution account numbers;

ii) Credit and debit card numbers, or equivalent;

iii) Credit and debit card expiry dates;

iv) Card Security Value (CSV) numbers;

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

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

vi) Balances of player accounts on the WBS.

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

i) Financial Institution PINs; and

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

7.5 Player Account Statements

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

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

7.5.3 Account statements must also include details of major wins.

7.6 De-activated Player Accounts

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

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

7.6.3 The Licensee must establish policies, standards and procedures regarding the treatment of retention of unclaimed monies and dormant accounts, and the WBS requirements at sections 4.6.1 - 4.6.4 of this document.

7.7 Player Loyalty

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

7.7.2 The player loyalty dataset must be able to be viewed and managed as a logically distinct dataset.

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

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

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

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

8
Wagering and Betting Transactions

This chapter sets out the Wagering and Betting transaction requirements that must be followed for operation in Victoria.

8.1 General

8.1.1 The specifications in this section are general and do not refer to specific types of wagering or betting. The intent is to cover Wagering and Betting transactions currently known and authorised by the Wagering and Betting Licence and related Agreement(s), and approved by the Commission, and provide the framework for future types.

8.1.2 Commission approval must be obtained for an Approved Betting Competition, Approved Betting Contingency, Approved Bet Type, or Approved Betting Event and will be considered on a case by case basis.

8.2 Transaction Logging

8.2.1 All Wagering and Betting transactions of significance must be logged by the WBS in accordance with sections 4.10.2 – 4.10.7.

8.2.2 The Commission will decide what consists of a transaction of significance on a case by case basis but must include:

i) Significant Events as per section 4.8;

ii) Wagering and Betting sells and cancels;

iii) Winning wagers paid, including refunds due to scratchings or abandonment;

iv) Wins added to player accounts;

v) Wagers and bets that are abnormal;

vi) Change of prize tables, odds, commissions, percentage or other payout selection; and

vii) Change of event status:

a) Start/stop wagering or betting;

b) Results entry/modification/confirmation;

c) Withdrawal/reinstatement of selections;

d) Events that are re-run;

e) Abandoned events; or

f) Alteration/override of event start time.

8.3 Placing Bets

8.3.1 The WBS must maintain a list of all active betting events available to a player.

8.3.2 The WBS must maintain a list of all Approved Bet Types available to a player.

8.3.3 The WBS must provide a user friendly approach to placing a bet, with all options and selections, including their order if relevant, clearly obvious to the customer.

8.3.4 The WBS must provide a clear indication to a customer that a wager has been accepted by the system, including full details of the actual bet accepted.

8.3.5 If the WBS rejects a wager, the system must provide a clear and meaningful indication to a customer of the reason(s) for the rejection of the wager.

8.3.6 The WBS must provide facilities for customer with a player account to search their complete history of all Wagering and Betting activity for a period of at least seven (7) years.

8.4 Cancelling Bets

8.4.1 The Licensee must obtain Commission approval of any method for a WBS operator to cancel a player's active bet(s).

8.4.2 In the event that the WBS allows a bet to be cancelled:

i) For a cash ticket that is cancelled, the customer must be refunded the amount of the original bet;

ii) For an account based wager, the player's account balance must be immediately updated with the amount of the bet that was cancelled; and

iii) All relevant pool(s) should have their component of the cancelled wager removed (subtracted).

8.4.3 The WBS may provide a cancellation period-of-grace to allow players sufficient time to cancel bets placed incorrectly.

8.4.4 If a cancellation period is offered in accordance with 8.4.3 the period of time must be short in duration and must end before an event has begun.

8.4.5 A late cancellation facility may be approved for use by the Commission provided there is the appropriate level of security and logging of the transaction.

8.5 Closing of Events

8.5.1 Upon the closing of an event the WBS must immediately prevent the placing of bets on the event and notify players still in session that the event is closed and the placing of bets on the event shall not be possible.

8.5.2 The Licensee must obtain Commission approval of any method within the WBS that allows an event to be re-opened.

8.5.3 Following circumstances when an event has been re-opened, the WBS shall immediately provide notification means to players that the event has been re-opened.

8.5.4 Any event that is reopened must be logged as a Significant Event.

8.6 Betting In-the-Run

8.6.1 The system must not allow betting in-the-run where not permitted by Legislation.

8.6.2 The Licensee must establish and maintain policies, procedures and standards in relation to how the WBS will handle events moving into a 'Betting In-the-Run' state.

8.6.3 The WBS must provide clear and meaningful indication that an event has entered the Betting In-the-Run stage.

8.7 Event Results

8.7.1 An event result must not be able to be entered into the WBS until the event is closed.

8.7.2 The position of all selections that may affect the result of a bet type associated with an event must be entered into the WBS.

8.7.3 The WBS must provide notification when an event has closed and the result of the event when it becomes available.

8.7.4 The WBS shall be able to modify an event result when circumstance permit up until the result has been confirmed, and the Licensee must obtain Commission approval of any such method.

8.7.5 Following circumstances when WBS results for an event have been modified, the WBS shall provide notification that the event result has been modified and calculate new dividends based upon the changed result.

8.7.6 The WBS must facilitate the ability to retrieve results and dividends on any closed event for a period of time as described in the Betting Rules.

8.7.7 Any modification of a confirmed event result must be logged as a Significant Event.

8.8 Dividend Calculation

8.8.1 Dividend calculation for pari-mutuel pools must not commence until the results for the event/pool are entered.

8.8.2 Where pools are shared with other totalisators, e.g. inter-state or Internet betting nodes, dividends should not be calculated unless all collations are received from all nodes. Policies, standards and procedures for overriding this rule are to be developed and approval for them obtained from the Commission.

8.8.3 For each pool for which a dividend is calculated, where possible, the WBS must maintain a record of dividend and settlement statistics regarding the monies involved in the calculation including, but not limited to:

i) Gross sales;

ii) Scratchings;

iii) Net sales;

iv) commission;

v) Jackpot amount in, if any;

vi) Winning units for each winning combination;

vii) Calculated dividend for each winning combination or an indication that a dividend could not be calculated;

viii) Jackpot amount out, if any;

ix) Fractions calculated, if any;

x) Subsidies calculated, if any;

xi) Rounding calculations;

xii) Total payout; and

xiii) Parlay wager statistics, including re-investments, where appropriate.

8.9 Winning Payments

8.9.1 Once an event result has been entered, dividends calculated and an appropriate Start Pay is issued in the WBS, the system must:

i) Make available for payment winning cash wagers of all confirmed dividends and refunds; and

ii) For account based wagers, credit winning wagers and refunds directly to the players account immediately or upon the next access to the account.

8.9.2 If parlay wagers were placed on the event,

i) A re-investment process must be carried out for transfer of all winning or refunded wagers, which are not the last leg of the formula, to the relevant selected pool; and

ii) The system must maintain statistics of all re-investments including any rounding that may have occurred.

8.10 Selection Withdrawal (Scratching)

8.10.1 The WBS must ensure that selections cannot be withdrawn if a Start Pay has been issued for any pool involving that selection. A Stop Pay must be performed first.

8.10.2 Selection withdrawal must lead to the cancellation of any results entered and hence any calculated dividends.

8.11 Fixed Prize Bet Types

8.11.1 This section refers to specific requirements for bet types where the payout is to be fixed at the time the bet is placed.

Current Odds Access

8.11.2 At all times the WBS must enable player access to all current odds for all available events and bet types.

Fixed Prize Bets

8.11.3 All requirements set out in 8.3 apply to fixed prize bets.

8.11.4 The WBS must provide fixed prize bet confirmation including the amount of the bet and the odds actually accepted by the system.

Limitation of Fixed Prize Liability

8.11.5 The WBS must implement the Betting Rules in circumstances where the Licensee attempts to reduce the potential liability in a single event, by means including but not limited to:

i) Prorating – abatement of large winners in an event when the overall payout liability is large. Note: Approval for prorating parameters must be obtained from the Commission;

ii) Liability Limits – fixed odds bets automatically reject if the liability for a selection would exceed a predefined limit established by the Licensee; and

iii) Partial bet acceptance or rejection – circumstances where the WBS only accepts part of a bet or totally rejects a bet, commonly followed by a change of the prize table.

Modification of Fixed Prize Payout

8.11.6 The WBS must provide, at the point of purchase, the Betting Rules stating the circumstances when it is permitted for the WBS to dynamically modify the payout table, e.g. a change of odds on an event.

8.11.7 The WBS must provide, at the point of purchase, players with immediate notification when the odds are changed.

8.11.8 Following changes to the odds, all subsequent access to the odds must display the latest version.

Fixed Prize Payout Adjustment

8.11.9 The WBS must make the Betting Rules available to the player and implement the Betting Rules regarding the circumstance(s) when fixed prize payouts are to be adjusted including but not limited to:

i) Dead heats;

ii) Withdrawn selections;

iii) Abandoned legs of multi leg wagers; and

iv) Prorating.

Spread Betting

8.11.10 If spread betting is catered for in the Betting Rules, the WBS must implement those rules including the calculation of winnings and losses, dependent upon the event outcome.

8.11.11 If the Betting Rules provide for a Stop Loss facility, the WBS must implement a means to limit losses for all spread betting wagers.

8.12 Pari-mutuel Event Types

8.12.1 This section refers to specific requirements for bet types where individual bets are gathered into pools.

8.12.2 The WBS must be able to report any change of commission for any bet type or pool.

8.13 Jackpots

Wagering and Betting Jackpots

8.13.1 Jackpot in the Wagering and Betting context means amounts of money that are not won, due to the absence of prescribed winners, and are carried forward into subsequent pools, generally of the same type.

8.13.2 If the Betting Rules cater for the carry forward of a pool or a component of a pool, e.g. when a pool has no winner, the WBS must implement the formula specified by the Rules, to determine the amount of money that is to “jackpot”.

8.13.3 If a pool or a component of a pool is to be carried forward, the WBS must transfer the “jackpot” to the subsequent pool as specified by the Betting Rules.

8.13.4 All Jackpot Out and Jackpot In monies are to be accounted for and documented. Refer also to section 8.8.

9 Customer Interface

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

9.1 Available Information

9.1.1 This section refers to requirements for information that is to be made available to WBS customers.

Race-day/Event Information

9.1.2 At a minimum, the following information must be available to customers concerning the race-day or events scheduled:

i) Schedule including events, times, pools, selection names;

ii) Prospective odds for simple pools;

iii) Pool grand totals;

iv) Current odds for fixed odds wagers;

v) Change of status including:

a) Scratchings and reinstatements.

b) Start and stop sell;

c) Results and change of results;

d) Dividends;

e) Start and Stop Pay;

f) Abandoned meetings, races, or pools; and

g) Race or event time change.

Bet Information

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

i) The totalisator or approved betting competition concerned;

ii) Date, time, selling location;

iii) Meeting, event/race(s), pool, time;

iv) Selection or combination of selections chosen, including selection names where practicable;

v) Unit bet;

vi) Total bet;

vii) Odds and prospective payout for fixed odds wagers; and

viii) Spread (for spread betting).

9.2 WBS Retail Terminal Wagering

9.2.1 This section refers to requirements relating to the use of WBS retail terminals to provide betting facilities to WBS customers.

Odds Displays

9.2.2 Wagering based in WBS premises, e.g. participating outlets or oncourse venues, will require odds displays and must provide at least the race-day/event Information described in section 9.1.2.

9.2.3 Odds display programs, for selecting content to the various display channels, must ensure that appropriate odds and status change information are shown in a timely manner.

9.2.4 Where Infield indicators are used in a race course environment, their update must be conducted in an accurate and timely manner.

Operator Entered Cash Betting

9.2.5 Operators at betting terminals may accept wagering transactions, bets, cancels and pays as a cash exchange.

9.2.6 Whenever a wager is placed, a unique ticket must be printed containing the information in section 9.1.3 and a unique serial number to identify the wager.

9.2.7 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 “forgeable”.

9.2.8 A means of cancelling cash wagers must be provided – refer to section 8.4

9.2.9 A means of paying winning or refunded cash wagers must be provided – refer to section 8.9.

9.2.10 Transactions at a WBS terminal involving WBS player accounts may be acceptable provided:

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

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

WBS Serial Numbers

9.2.11 All serial numbers used in the WBS must be uniquely identifiable and created by a secure and tamper proof algorithm.

Self Service Terminals (SST)

Account Based SST Wagering

9.2.12 When bets are made against an existing player account, it is not necessary to print a cash ticket receipt for any wager but the wager information of section 9.1.3 and the account balance after the transaction must be made immediately available.

Cash Exchange SST Wagering

9.2.13 Alternatively, “cash exchange” wagers may be made by first inserting money into the SST via banknote, coin or debit card.

9.2.14 In this instance a cash ticket receipt must be printed for each wager accepted by the system. In addition, all of the requirements of sections 9.2.6 - 9.2.10 must be met.

9.3 Telephone Betting

9.3.1 This section refers to requirements relating to the placing of wagers for WBS customers by WBS operators where communication is made via telephone calls.

9.3.2 All wagers must be placed against an account but only after access to an existing account with account ID and appropriate security control e.g. PIN.

9.3.3 When bets are made, the wager information of section 9.1.3 and the account balance after the transaction must be made immediately available and relayed via the telephone to the customer.

9.3.4 There must be a means for WBS operators to view all wagers placed against a WBS customer’s account from the operator’s terminal.

9.3.5 There must be a means to cancel bets placed against the account from the operator’s terminal.

9.3.6 The customer must be able to request the race-day/event information of section 9.1.2 which would be displayed on the operator’s terminal and relayed over the telephone to the customer.

9.3.7 All conversations involving telephone betting wagers must be voice recorded and the recordings stored for a minimum of 2 years.

Unassisted Phone Betting

9.3.8 This section refers to requirements relating to WBS customers placing their own wagers via telephone calls via Interactive Voice Response (IVR) or touch tone phone (DTMF).

9.3.9 There must be a menu system in place to enable the customer to log-in to the WBS system, request information and place wagers.

9.3.10 As bets are made the wager information of section 9.1.3 and the account balance after the transaction must be read back to the customer over the telephone to the customer.

9.3.11 There must be a means of requesting details of wagers placed against the account.

9.3.12 There must be a means to attempt to cancel bets placed against the account.

9.3.13 It must be possible to access the race-day/event information of section 9.1.2 upon request through the relaying of voice information by the WBS system over the phone.

9.3.14 It may be acceptable for a phone betting customer to login to the account via IVR or DTMF and then be transferred, or elect to be transferred, to an operator for betting transactions.

9.4 Online Betting

9.4.1 This section refers to requirements relating to WBS customers placing their own wagers via terminals connected to communication channels such as the Internet or digital television.

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

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

9.4.4 As bets are made the wager information of section 9.1.3 and the account balance after the transaction must be displayed to the customer on the input device e.g. screen.

9.4.5 It must be possible to access the race-day/event information of section 9.1.2 with response to be displayed on the input device.

9.5 Bulk File Transfer

9.5.1 This section refers to requirements relating to WBS customers placing their own wagers via a bulk transfer method such as FTP and is additional to those from above depending upon which medium is used.

9.5.2 A log must be maintained for all wagers that are attempted to be placed via the bulk transfer including success or failure of each wager and the amount for each successful wager.

9.5.3 A bulk wager that would cause the account balance to go negative must not be accepted.

9.5.4 Methods must be in place to prevent bulk wager processing from degrading the system performance.

10 External WBS Requirements

This chapter sets out the System requirements that must be met for all WBS activities carried out in Victoria in conjunction with one or more external Wagering and Betting systems.

10.1 Introduction

10.1.1 This section refers to requirements for the circumstances where the WBS communicates with external systems to provide shared/common pools in any of the following configurations:

i) The WBS is the "host system" receiving collations and/or wagers from one or more external systems; or

ii) The WBS is a "guest system" passing its collations and/or wagers to a "host system".

10.2 Communications with External Wagering Systems

10.2.1 Communications with an external wagering system must meet the requirements of section 5 of this document.

10.3 Wagering Process – Bets Held on External Systems

10.3.1 This section refers to requirements for event types or bet types where details of bets placed through the WBS are forwarded to an external Wagering and Betting system which controls the wagering, processes and results, and determines winning wagers.

10.3.2 Bets placed on the WBS must receive clear acknowledgment of acceptance or rejection by the external Wagering and Betting system.

10.3.3 Cancellation requests from the WBS must receive clear acknowledgment of acceptance or rejection of the cancellation by the external wagering system.

Account Based Wagers and External Systems

10.3.4 If the cost of the wager is determined by the external system, there must be a positive confirmation sequence in place to enable the player to accept the bet cost and the WBS to determine that there are enough funds in the player's account to meet the wager cost.

10.3.5 The account balance is not to be debited by the WBS until final confirmation is received from the external wagering system.

10.3.6 The account balance for a cancellation is not to be credited by the WBS until final confirmation is received from the external wagering system including the amount of the cancel.

Winner Update

10.3.7 When results are entered and confirmed on the external wagering system, each winning wager placed from the WBS must be transferred from the external system to the WBS with the amount of the win.

10.3.8 All winning wagers and their winning amounts are to be handled as per section 8.9.1 of this document.

10.4 Pari-mutuel Wagering Information

10.4.1 This section refers to the exchange of wagering information between the WBS and external Wagering and Betting systems whether the WBS is a host or guest system.

10.4.2 Guest wagering systems involved in pari-mutuel wagering must periodically pass their relevant current collations and pool betting totals for all active pools to the host system.

10.4.3 A host wagering system which provides pari-mutuel wagering facilities must periodically pass the current collations for all relevant active pools to the guest system(s).

10.4.4 The host wagering system must immediately pass change of event status information to the guest system(s) whenever any change occurs including, but not limited to:

i) Withdrawn or reinstated selections;

ii) Altered event starting time;

iii) Event closed or open;

iv) Results entered or modified;

v) Results confirmed; and

vi) Event abandoned.

10.4.5 When a guest system receives notification from the host system of event closure, all pools that are associated with that event must be immediately closed for sales.

10.4.6 When a guest system receives notification from the host system of event results, all relevant final collations for pools that are associated with that event must be immediately forwarded to the host for the purpose of dividend calculation. Refer to section 8.8.2 for handling of circumstances where not all relevant collations are received by the host system.

10.4.7 The host system must forward to the guest systems all dividends as they become available including their final status.

10.5 Settlement with External Systems

10.5.1 A host wagering system which provides pari-mutuel wagering facilities must calculate and maintain for each guest system and overall, the dividend and settlement statistics in section 8.8.3.

10.5.2 Where appropriate, the WBS, if a guest system, must independently calculate and maintain the dividend and settlement statistics in section 8.8.3.

10.5.3 At the end of a racing period, a settlement process between the host and all guest systems must occur and be agreed.

10.5.4 If fractions and subsidies are to be shared between the WBS and external system(s), the process for determining the share must be formally documented and approval obtained for the process from the Commission. The WBS must maintain statistics of fractions and subsidies shared between all systems when the WBS is acting as the host.

10.6 Fixed Price Wagering Information

10.6.1 A host wagering system which provides fixed price wagering facilities, where the odds and prize table can be dynamically changed, must immediately pass the current odds to all guest system(s) whenever any odds are changed.

10.6.2 All change of status information, as per section 10.4.4, must be passed from the host system to the guest system(s) as changes occur.

10.7 Restart and Recovery

10.7.1 The process of all Wagering and Betting activities between Wagering and Betting systems is not to be adversely affected by restart or recovery of any computer system or network or communications infrastructure. Wagering and Betting transactions must not be lost or duplicated because of recovery of one system or the other.

10.7.2 Upon restart or recovery, the WBS must immediately synchronise the current status of all transactions, data and configurations identified in section 10.4 with the external system(s).

10.8 Communication with External Non-Wagering Systems

10.8.1 Communication with external systems for non-wagering purposes must not interfere or degrade normal WBS functions.

10.8.2 Where the communication with external non-wagering systems is for a critical purpose, e.g. transfer of a racing schedule, the communication requirements of section 5 must apply.

11 Betting Exchange System Requirements

This chapter sets out the System requirements that must be met for all WBS activities carried out through a licensed Betting Exchange in Victoria.

11.1 General

11.1.1 A Betting Exchange is recognised as an on-line medium where an individual player makes bets not with a bookmaker but with other individual players. Players can choose to either back an outcome as you would normally with the bookmakers, they can play the role of the bookmaker and 'lay' an outcome or they can simply 'trade' the betting market.

11.1.2 Commission approval must be obtained for all events to be made available through the medium of a Betting Exchange (in the same way as an Approved Betting Event).

11.1.3 A Betting Exchange is a part of the overall WBS and therefore must meet all the requirements for the WBS in this document.

11.2 Betting Exchange Requirements

11.2.1 The remainder of this section details the specific technical requirements applicable to the Betting Exchange component of the WBS. The Licensee must ensure the WBS meets these requirements in order to operate a Betting Exchange facility.

11.2.2 The Licensee must establish and maintain policies, procedures and standards to deter, prevent and detect collusion and cheating.

11.2.3 The WBS must retain a record of relevant activities to facilitate investigation and be capable of suspending or disabling player accounts.

11.2.4 The WBS must facilitate the ability to suspend Wagering and Betting activities on events both automatically and through manual intervention.

11.2.5 The Licensee must seek approval from the Commission for allowing the use of automated gambling software on the betting exchange.

11.2.6 If the Betting Rules allow the use of automated gambling software on the Betting Exchange, the WBS must make information available to players that automated gambling software may be being used by other players using the Betting Exchange.

11.2.7 Players must have a valid player account in order to use the Betting Exchange and player accounts must meet the requirements in section 7 of this document.

11.2.8 Each Wagering and Betting transaction processed by the Betting Exchange must be linked to a single valid and unique player account.

11.2.9 The WBS must record every transaction processed by the Betting Exchange.

11.2.10 Individual players participating in the Betting Exchange must be anonymous to each other.

11.2.11 The WBS must be capable of making all transactions available to sports and racing governing bodies in a timely manner when instructed by the Commission.

11.2.12 The WBS must be capable of meeting the Betting Rules relating to unmatched wagers.

12 Simulated Racing Event System Requirements

This chapter sets out the System requirements that must be met for all Simulated Racing Event activities carried out by the licensee in Victoria.

12.1 General

12.1.1 A Simulated Racing Event is recognised as a computer generated horse, harness or greyhound 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.

12.1.2 Approval must be obtained from the Commission for all Simulated Racing Events.

12.1.3 Simulated Racing Events are a part of the overall WBS and therefore must meet all the requirements set out for the WBS in this document.

12.1.4 The remainder of this section details the technical requirements for the Random Number Generator used to determine the outcome of a Simulated Racing Event.

12.2 Random Number Generator (RNG)

12.2.1 The Commission requires the use of a random number generator (RNG) for the selection of the results of Simulated Racing Event products.

12.2.2 The RNG algorithm and its use must be submitted to the Commission as part of the request for WBS approval.

12.2.3 The RNG must be isolated from the rest of the Simulated Racing Event system. This isolation may be achieved by:

i) A physically separate RNG unit; or

ii) RNG software that is contained within the Simulated Racing Event computer system but is logically isolated from the rest of the software.

Physically Separate RNG Unit

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

12.2.5 Approval for the physical security of the RNG must be obtained from the Commission.

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

12.2.7 The RNG must comply with specific requirements for Electromagnetic interference as detailed in 4.1.5.

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

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

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

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

Logically Separate RNG

12.2.12 If the RNG is to be logically separated from the Simulated Racing Event software, the RNG software must be totally independent of the rest of the Simulated Racing Event software.

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

12.2.14 Communication with the Simulated Racing Event software must be only through controlled means in the same manner as if it were a physical connection.

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

RNG Software Storage

12.2.16 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, must be approved by the Commission.

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

Duplicated RNG Units

12.2.18 The RNG unit must be duplicated - i.e. there must be at least two RNG's available during normal operation.

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

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

12.2.19 The Commission does not require random selection of a RNG device.

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

Record of Simulated Racing Event Selections

12.2.21 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.

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

12.2.23 The recorded output should show at least:

i) Date;

ii) Time;

iii) The Simulated Racing Event number;

iv) The numbers drawn;

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

vi) Other security information if available.

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

12.3 Communication Between RNG and WBS

Method of Communication

12.3.1 Approval from the Commission must be obtained for the methods of communication from the RNG to the WBS. If serial communication is to be used, refer to section 5 of this document.

Security of Connection of RNG Device

12.3.2 The method of transferring data between the RNG and the WBS computer is to be secure and tamper proof, whether by physical means from a separate unit or logical means within the Simulated Racing Event computer system(s).

12.3.3 The WBS and the RNG devices are to be designed to reduce the chance of "rogue devices" communicating false results to the WBS host.

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

12.4 Mathematical Requirements of the RNG

12.4.1 Where a Simulated Racing Event product result is determined by a Random Number Generator, the RNG is a vital component and approval for its implementation and use must be obtained from the Commission.

12.4.2 For RNG requirements, refer to the Australian/New Zealand Gaming Machine National Standard.

12.5 RNG Test Modes

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

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

12.6 Software RNG versus Hardware RNG

12.6.1 The Commission 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.

12.6.2 While the Commission 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.

12.7 Chance Simulated Racing Event Behaviour

12.7.1 The following rules apply to the use of random number generators relative to chance Simulated Racing Event behaviour.

Chance Simulated Racing Event Behaviour to be Uncorrelated

12.7.2 Events of chance within games must be independent of (i.e. uncorrelated with) any other events within the Simulated Racing Event or any events within previous games.

Chance Simulated Racing Event Behaviour not to be Influenced

12.7.3 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

12.7.4 Events of chance within games must not be automatically influenced in any way by recent history or other statistics.

Random Number Selection Sequence

12.7.5 The numerical values from the RNG used to determine chance 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 way.

12.7.6 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 Simulated Racing Event Behaviour to be Frozen

12.7.7 Prior to the commencement of each Simulated Racing Event, all random behaviour to be used during a Simulated Racing Event is to be fully determined and frozen.

12.7.8 This requires that all random numbers (including random decisions, random events or any other random behaviour) to be used during the course of the Simulated Racing Event are generated and recorded prior to the start of the Simulated Racing Event.

No Subsequent Decisions

12.7.9 Subsequent to the commencement of a Simulated Racing Event, no subsequent actions or decisions may be made that would change the behaviour of any of the events of chance within the Simulated Racing Event other than player decision.

Chance Simulated Racing Event Behaviour to be Recorded

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

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

Variable Odds Selections

12.7.12 If the Simulated Racing Event offers variable odds, selections must be picked in inverse proportion to the announced odds.

12.7.13 Odds for all bet types for an event must be directly proportional to the host odds for the event e.g. the Win odds.

12.8 Other Uses of RNG Prohibited

12.8.1 The “draw” RNG must not be used for any purpose other than the “official” use as identified by the rules of the Simulated Racing Event product.

12.9 Verification of the RNG Device

Software Functionality

12.9.1 For the RNG requirements for software functionality, refer to section 6.7.

Maintenance of Statistics

12.9.2 Simulated Racing Event product types must maintain a record for each event played and calculate “reasonableness” statistics on the results of the event in an attempt to identify and warn the WBS operator of possible non-random performance.

13
Testing Requirements

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

13.1 Inspection and Testing

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

13.1.2 The Licensee must establish and maintain policies, procedures and standards for quality assurance and control, equivalent to ISO900, 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) Usability, including ease of use for customer facing devices and graphic user interfaces (GUI);

v) Accessibility, including consideration of World Wide Web Consortium (W3C) standards, or equivalent;

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 Commission.

13.1.3 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

13.1.4 A Tester must work with the Licensee to undertake an evaluation of the WBS covering aspects including but not limited to:

i) Compliance with the relevant Rules;

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

iii) Matrix of Wagering and Betting products to selling channels;

iv) Accuracy and consistency in the display of information;

v) Functional integrity of communication protocols in use;

vi) Regulatory reporting;

vii) Licensee, participating outlets and/or customer access to the WBS;

viii) Integrity of player accounts;

ix) Integrity of user accounts; and

x) Integration or deployment of new technologies.

Facilities for a Tester

13.1.5 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 Commission accordingly.

Test Environment

13.1.6 The Licensee must ensure that upgrades to the WBS and associated WBS Equipment 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.

13.1.7 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 Commission.

13.1.8 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.

13.1.9 The test system must be able to interface to participating outlets.

Failure Modes and Recovery Testing

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

i) Failure of a WBS power supply;

ii) Total power failure of a WBS component or the primary site;

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

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

iii) Verifying there is no single point of failure;

iv) Individual server capability to sustain persistent load;

v) Guaranteed messaging;

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

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

viii) Failure of WBS I/O channels;

ix) Failure of links with remote interface points; and

x) WBS operator error, including but not limited to invalid data entry.

13.2 System Testing Requirements

Testing Requirements and Tester Recommendation

13.2.1 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 Manufactures, Suppliers and Testers as defined in the Act.

13.2.2 A Tester recommendation is required on:

i) The system integrity and reliability;

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

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

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

Associated Systems Requirements

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

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

Submission Requirements

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

i) Background of the WBS;

ii) Purpose of the submission

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

iv) Tester recommendation of the WBS in accordance with above requirements;

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

vi) List of all software versions and associated CRCs;

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

viii) Associated systems that are connected to the WBS;

ix) A WBS Baseline Document; and

x) A Network Policy Document (if applicable).

Environmental Testing

13.2.6 Suppliers of WBS equipment are to provide information as to the range of environmental extremes at which WBS Equipment 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.

13.2.7 The Commission requires the equipment to run within the equipment's own environmental specifications.

14 Submission Requirements

This chapter sets out the information types to be submitted relevant to the WBS for operation in Victoria

14.1 General

14.1.1 The Licensee must provide all relevant WBS policy, standard and procedure documentation for assessment by the Commission.

14.2 Event Wagering

14.2.1 The Licensee must provide details of all event wagering types to be provided including description of the events and bet types, rules, etc.

14.2.2 In relation to event details provide in accordance with 14.2.1, the Licensee must provide descriptions on how results are selected for these events.

14.2.3 The Licensee must provide descriptions of any links to external computer systems participating in the event wagering.

14.3 Player Information

14.3.1 The Licensee must provide player registration details.

14.3.2 The Licensee must provide descriptions of how player verification information is to be protected from unauthorised access.

14.3.3 The Licensee must provide details of player authentication.

14.3.4 The Licensee must provide details of the player exclusion and bet limit mechanisms.

14.3.5 The Licensee must provide descriptions of how player registration and account information is to be protected from unauthorised access.

14.3.6 If the proposed WBS is to include a Player Loyalty scheme, the Licensee must provide details of the Player Loyalty scheme and associated rules.

14.4 Communications

Authentication and Encryption

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

14.4.2 The Licensee must provide details of the encryption to be used during Wagering and Betting:

i) Encryption algorithms;

ii) Size of encryption keys;

iii) Key exchange procedure at session start-up;

iv) Subsequent key exchanges; and

v) Details of any information that is not encrypted for transmission.

WBS Internal Network Architecture

14.4.3 The Licensee must provide details of the proposed architecture of the internal production network to be used to supply Wagering and Betting facilities:

i) Network topology;

ii) Devices used to create the network; and

iii) Controls to prevent unauthorised modification to device configuration.

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

14.4.5 The Licensee must provide details of any remote connections (e.g. Internet, wide area network, and dial-up) used to support Wagering and Betting operations.

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

14.4.7 The Licensee must provide details of operator consoles, including:

i) Location of operator consoles in relation to the WBS.

ii) Protocols used by operator console connections.

iii) Access controls on operator console connections to the WBS.

iv) Authentication and encryption used by operator consoles.

v) Controls to prevent eavesdropping on communications between operator consoles and the WBS.

vi) Controls to prevent unauthorised use of operator consoles.

14.4.8 The Licensee must provide a list of all non-production systems and third party systems that will connect to the WBS.

14.4.9 For each external system provided in relation to 14.4.8, the Licensee must provide:

i) The connection method;

ii) Details of the information to be transferred in each direction;

iii) The entity that initiates the information transfer;

iv) The protocol used to perform the transfer;

v) The controls in place to prevent access to other information on the WBS;

vi) The controls in place to prevent unauthorised use of the connection; and

vii) The controls in place to prevent eavesdropping on communications between non-production systems and the WBS.

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

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

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

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

i) The physical location of the network management system;

ii) The class of personnel authorised to use network management system;

iii) The locations from where network management functions can be executed;

iv) The network management protocol;

v) The devices to be managed on a read only basis;

vi) The devices to be managed on a read/write basis;

vii) The controls in place to prevent unauthorised access to network management functions;

viii) The controls in place to audit the use of network management functions;

ix) The controls in place to detect unauthorised connections to the network; and

x) The controls in place to detect connection of unauthorised equipment to the network.

14.4.14 The Licensee must provide descriptions of the locations and physical and logical security arrangements associated with Domain Name Servers within the internal production network

Third Party Connections

14.4.15 The Licensee must provide description details of all connections to third party organisations.

14.4.16 The Licensee must provide evidence that the hardware and software to be used for the connections to financial institutions and for the conduct of transactions to and from the WBS is secure, reliable and auditable.

14.4.17 The Licensee must provide details of the tests conducted and results obtained in gaining certification and approval as described in 14.4.16

WBS Host Computers

14.4.18 The Licensee must provide an overview of the WBS design.

14.4.19 The Licensee must provide a functional specification of the WBS.

14.4.20 The Licensee must provide detailed WBS design documents.

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

i) Hardware platform;

ii) Operating system;

iii) Applications;

iv) Audit subsystem;

v) Duplication strategy;

vi) Disk subsystem;

vii) Magnetic back-up facilities;

viii) Physical security;

ix) Login security;

x) Power requirements; and

xi) Environmental condition requirements.

14.4.22 The information requested in relation to 14.4.21 applies also to other WBS Equipment to be used in the WBS computer environment. This should include such devices as:

i) Front ends;

ii) Firewalls;

iii) Operator consoles (local and remote);

iv) Remote controllers;

v) Remote access servers;

vi) Multiplexing equipment;

vii) Switching equipment;

viii) Monitoring equipment;

ix) Routers; and

x) Repeaters.

14.4.23 For each WBS component and associated equipment that is to be implemented, the Licensee must provide a detailed schedule of the planned implementation. This should include dates for the following:

i) First access to the WBS computer system;

ii) Access to the "final" WBS computer system;

iii) First access to each piece of individual equipment;

iv) Final access to each piece of individual equipment

v) Expected date when the Licensee's testing and QA has been completed and formal acceptance testing might begin; and

vi) Planned date for live operation.

14.4.24 The Licensee must provide descriptions of where and how information is stored throughout the system.

14.4.25 The Licensee must provide what statistics are stored by the system for each separate end player device type.

14.4.26 The Licensee must provide detailed descriptions of its password protection systems and associated algorithms utilised by the system.

14.4.27 The Licensee must provide a description of the method of transaction logging used.

14.4.28 The Licensee must provide details explanations of the situations during which encryption of data files will be employed.

14.4.29 Where data files encryption is to be employed, the Licensee must provide the following information:

i) Description of the algorithm;

ii) Theoretical basis of the algorithm;

iii) Results of any analyses or tests to demonstrate that the algorithm is suitable for the intended application;

iv) Rules for selection of keys; and

v) Means of setting and protecting keys.

14.4.30 The Licensee must provide a description on how self-monitoring is to be implemented.

WBS Software

14.4.31 The Licensee must provide the source software for the WBS software.

14.4.32 The Licensee must provide a description of how the each of the seven points for software verification detailed in 6.7.12 is to be achieved.

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

WBS Operations

14.4.34 The Licensee must provide details of each class of account required to operate the WBS in a production environment (e.g. system administrator, operator, hotline, network support).

14.4.35 For each class of account provided in relation to 14.4.34, the Licensee must provide details of the privileges required to perform the duties associated with that account.

14.4.36 The Licensee must provide details of the physical location of each component of the WBS, including the location of staff.

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

14.4.38 The Licensee must provide copies of all standard reports produced by the WBS and describe how these are generated, including details of any reconciliation of reports.

15
Related Documents

Document Title	Version
Australian/New Zealand Gaming Machine National Standard	V10.0
Victorian Appendix to the Australian/New Zealand Gaming Machine National Standard	V10.0
Wagering and Betting Licence	Unassigned
Wagering and Betting Agreement	Unassigned

End of Document