THE RICE MARKETING BOARD FOR THE STATE OF NEW SOUTH WALES

COMPUTING SECURITY POLICY

Version	Author	Date Approved by Board
2009-1	Gillian Kirkup	24 March 2010
2017	Carol Chiswell	12 May 2017

THE RICE MARKETING BOARD FOR THE STATE OF NEW SOUTH WALES
COMPUTING SECURITY POLICY

1. Purpose
This document describes the Computing Security Policy of the Rice Marketing Board for the State of NSW (the Board). It establishes guidelines and responsibilities to protect the information assets of the Board that are associated with the provision of Information Services.

2. Scope
The Computing Security Policy document specifies what is required to achieve a secure environment to protect the Board's information. For information on how this policy will be implemented, please refer to the Computing Security Procedures. This Policy is applicable to the employees, Members, contractors, consultants, and temporary workers employed by the Board, including those workers affiliated with third parties who access the Board's computer networks. This Policy applies to security measures relating to computerised systems, including all types of media and systems. Please refer to the Board's Records Management Policy for information on the retention and storage of documented information.

3. Responsibility
This policy is to be reviewed by the Board annually and is managed and implemented by the Board's Secretary.

4. Communication
In order that all Board Members and employees are aware of this policy, the policy will be made visible in the following ways:

- Current employees including Board Members - Revisions are approved at board level and then communicated to employees by the Board's Secretary.
- New Board Members and employees – This Policy is included as part of the induction program to ensure all employees and Members are aware of the policy.
- Contractors, Consultants and other third parties – The Board Secretary is responsible for ensuring that each contractor, consultant or other third party is aware of the policy.

5. Background
Information and Information Systems are important assets of the Board. These assets include data and software, whether internally developed or acquired from outside sources, and computer resources including devices and systems used to process and maintain information. The Board needs accurate, timely, relevant, and properly protected information to operate effectively. The Board takes steps to ensure that the information and information systems are properly protected

from a variety of threats. This document describes the key areas of the Computing Security Policy.

6. Methods

Various methods are required to secure the Board's information and Information Systems which includes using access control, physical security, data protection, security incident handling and compliance.

6.1 Access Control

6.1.1 User Access Management

Access rights to information services are controlled through the use of passwords to prevent unauthorised computer access. This covers all stages in the life cycle of user access, from the initial registration of new users to the final deregistration of users who no longer require access to computer services.

6.1.2 User Responsibilities

For effective security and to prevent unauthorised access, it is the responsibility of authorised users to maintain effective access controls.

6.1.3 Network Access Control

Connections to the Board's network are controlled to protect information systems. This ensures that connected users and computer services do not compromise the security of any other networked services and that the connecting systems are sufficiently protected against network borne threats.

6.2 Physical Security

The server containing sensitive data, is located in a locked office only accessible to authorised personnel. Computer facilities supporting critical or sensitive data are housed in secure areas to prevent unauthorised access, damage and interferences to computer services. These facilities are physically protected from unauthorised access, damage or interference. An Uninterrupted Power Supply (UPS) unit is used to safeguard the electrical supply.

6.3 Data Protection

6.3.1 Virus Protection and Client-side Firewall

To safeguard the integrity of software and data, precautions are employed to prevent, detect and report the introduction of viruses and hacking threats.

6.3.2 Backups

A proper backup strategy is employed to protect important data and programs in the event of errors, disasters, or hardware or software failure.

6.3.3 Development and Support Environments

Project and support environments are strictly controlled to maintain the security of applications and data. All proposed changes are reviewed to ensure that they do not compromise the security of either the system or the operating

environment. To ensure that security is built into IT systems, security requirements are identified and approved by the Board prior to the development of or changes to IT systems. Appropriate security controls, including audit trails are designed into the application systems.

6.3.4 Intellectual Property Rights and Disclosure of the Board's Information

Disclosure rules and intellectual property rights are used to protect the Board's information.

6.4 Security Incident Handling

To handle a security incident refer to the Disaster Recovery Plan to minimise disruption, find the cause of the security incident, fix the problem and stop it from occurring again.

6.5 Compliance

Compliance with this security policy is essential to ensure the success of the policy and the protection of the Board's information and Information Systems. System users are made aware of the implications if they do not comply with the policy.

7. Implementation

7.1 Access Control

7.1.1 User Access Control

Signed Forms Required for Issuance of User ID

Staff are required to sign a confidentiality agreement as part of the process of being given a User ID.

7.1.2 Issuance of User ID to Non-Board staff

In the event where non-Board staff need access, the sponsoring group within the Board are required to define the level of access as well as the amount of time the account is to be available. The account will be set to expire at close of business on the nominated date unless a revised date is agreed.

7.1.3 Determining Security for Corporate Applications and Systems

Access to all systems and applications have user privileges defined by the Board's Secretary.

The Board's Responsible Computing Policy defines acceptable and unacceptable computing uses and practices within the Board's computing environment.

8. Termination of Staff

8.1 Changing Physical Access Control Codes

In the event that a staff member's employment with the Board is terminated, all physical security access codes known by the staff member are deactivated or changed.

8.2 Confidentiality of the Board's Documentation
The Board's documentation is confidential, and is not taken anywhere when an employee, consultant, or contractor completes their service with the Board.

9. User Responsibilities

9.1 Single User ID
Staff members have only one User ID across all the systems unless there are specific requirements to the contrary. Generic or shared User IDs are strongly avoided, and clearly documented as to why they are necessary when this is required.

9.2 Staff Responsible for all Activities Involving Personal User IDs
Staff members are responsible for all activities performed with their personal User IDs. User IDs are not utilised by anyone but the individuals to whom they have been issued.

9.3 Password Sharing Prohibition
Regardless of the circumstances, staff are prohibited from revealing their passwords to anyone else. To do so exposes the authorised person to responsibility for actions that the other party takes with the password.

9.4 Leaving Systems Unsecured
Staff members are not to leave their workstations without either first logging out or securing them.

9.5 Suspected Disclosure Forces Password Changes
All passwords are promptly changed if they are suspected of being disclosed or known to anyone else.

9.6 Password Security
Staff members are prohibited from writing down their passwords as they may be left in a place where others might discover them.

9.7 Storage of Passwords in Readable Form
Staff members are prohibited from storing passwords in batch files, automatic log-in scripts, software or terminal function keys.

9.8 Display and Printing of Passwords
Where practical, the display and printing of passwords is suppressed, such that no indication of the password is echoed on the screen.

9.9 Periodic Forced Password Changes
All staff members are automatically forced to change their passwords at least once every ninety days.

9.10 Password Characteristics

Passwords are more difficult to guess if they contain at least one alphabetic and one non-alphabetic character. Non-alphabetic characters include numbers (0-9) and punctuations. The use of control characters and other non-printing characters is discouraged because they can cause unexpected results. Passwords are a minimum of 6 characters in length.

9.11 End-User access to Operating System Prompts
Access to the Operating System Prompts on the Board's Corporate Systems is restricted to authorised staff only. All other staff are restricted to menus or authorised applications.

9.12 Changing Vendor Default Passwords
All vendor-supplied default passwords are changed before any computer or communications system is used for Board's business.

10. Network Access Control

10.1 Modems on Workstations Connected to Internal Networks
Staff members are prohibited from connecting dial-up modems to workstations without explicit approval from the Board's Secretary.

10.2 Approval Required for Systems accepting incoming Dial-up Calls
Board staff members are prohibited from establishing any communications systems which accept incoming dial-up calls unless these systems have first been approved in writing by the Board.

10.3 Network Access Verification
All staff members are required to have their identity verified with a User ID and a password or by other means which provide equal or greater security prior to being permitted to use the Board's computers connected to a network.

10.4 Maximum Permissible Password Attempts for Remote Users
If a computer user coming over a VPN or dial-up line has not provided a correct password after three consecutive attempts, the connection is immediately terminated and the involved User ID suspended.

10.5 Real-Time Internal Network Connections
All real-time external connections to the Board's internal networks and/or multi-user computer systems is passed through an additional access control point (e.g. a firewall) before users can reach a log-in banner.

10.6 Publication of Computer-Related Contact Numbers
Information regarding access to the Board's computer and communication systems, such as VPN configuration and dial-up modem phone numbers, is confidential. This information is kept secure and is NOT posted on electronic bulletin boards, listed in telephone directories, placed on business cards, or otherwise made available to unauthorised parties.

10.7 Internal Network Addresses Not Publicly Released
The internal addresses, configuration, and related system design information for the Board's networked computer systems is restricted such that both systems and users outside the Board cannot access this information without explicit approval from the Board's Secretary.

11. Auditing

11.1 Required Retention Period of Logs
Logs containing computer security relevant events are retained online for at least three (3) months. During this period, such logs are secured such that they cannot be modified. These logs are important for error correction, forensic auditing, security breach recovery, and related efforts. These logs are archived prior to removal from the system.

12. Physical Security

12.1 Secure Areas
IT facilities supporting critical or sensitive data are housed in secure areas to prevent unauthorised access, damage and interferences to IT services. Supporting facilities such as electrical supply and cabling infrastructure are also safeguarded.

12.2 Environmental Controls
Rooms containing the Board's computer equipment have a controlled environment that is optimal for computer systems and equipment to ensure continuous operation. Protection systems (e.g. fire suppression and power generation) are employed to limit disruptions due to fire or natural disasters.

12.3 Approval for Disposal of IT Equipment
The disposal of any IT equipment is approved by the Board.

12.4 Destruction/Concealment of Information before Disposal
Before computer magnetic storage media is sent for trade-in, or disposal, all the Board's sensitive information is destroyed or concealed according to approved methods.

12.5 Physical Security Measures for Computers & Communications Systems
All reasonable care is taken to restrict physical access by unauthorised personnel to computer and communication systems.

12.6 Computer Equipment Identifications
All the Board's computer and communications equipment is recorded in the asset register including serial numbers.

13. Data Protection

13.1 Virus Protection

13.1.1 Test for Viruses
If a virus, worm, or Trojan horse is suspected or present on software and/or files, the Board's Secretary is required to act immediately to mitigate their impact by contacting the Board's authorised service agent. Computer viruses spread quickly and need to be eradicated as soon as possible to limit serious damage to computers and data.

13.1.2 Only Use Authorised Software
No unauthorised software is installed, stored or used on any of the Board's computer systems. Third party software is approved by the Board before it is installed onto Board computer systems.

13.1.3 All User Involvement with Computer Viruses Prohibited
Staff members are not allowed to intentionally write, generate, compile, copy, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software.

13.1.4 Operation of Virus Checking Programs
Virus checking programs approved by the Board are continuously enabled on all local area network (LAN) servers and networked personal computers (PCs). The Board's Secretary is responsible for ensuring that the virus update patches are applied on a regular basis and that the Board's virus protection methodology and processes remain current.

14. Backups

14.1 Backup of PC Data
Data stored on the LAN file server is backed up on a regular basis, and this process is the responsibility of the Board's Secretary.

14.2 What Data to Backup and Minimum Backup Frequency
All sensitive, valuable, or critical information resident on the Board's systems is periodically backed-up. As a minimum, back-ups for all end-user server-based files is performed by procedures starting at a specified time each business day.

14.3 Development and Support Environments
14.3.1 Security Requirements Specification
Before a new system is developed or acquired, relevant security requirements are identified and approved by the Board. It is cheaper and more effective to incorporate security into the design and development stages rather than as a "add on" at a later stage. Consideration is given to an appropriate balance between security and other objectives, for example, ease-of-use, operational simplicity, ability to upgrade and acceptable cost.

14.3.2 Access to Production Business Data by Development Staff
Where possible, development staff can only access the production business data in “read-only” mode to investigate problems.

15. Intellectual Property Rights and Disclosure of the Board’s Information

15.1 Disclosure of Security Systems Information
Staff are prohibited from disclosing to any unauthorised persons outside the Board, details of the security systems that are in use or the way in which they are implemented.

15.2 Disclosure of Information System Vulnerabilities
Specific information about Information System vulnerabilities, such as the details of a recent system break-in, is not distributed to unauthorised persons.

15.3 Disclosures of Corporate Information
All disclosures of the Board’s corporate information to third parties are accomplished via a signed confidentiality agreement unless otherwise required by law. The confidentiality agreement includes restrictions on the subsequent dissemination and usage of the information. Any such dissemination of corporate information is approved by the Board.

15.4 Disposal of Printer Information
When printed matter is disposed of staff are required to consider the nature of the information in the document and dispose of it appropriately. Shredders and security bins are available for sensitive documents containing financial or personal information.

15.5 Identification of Production, Test, Training and Development Data
Production, test, training, and development data is easily identifiable as such on any printed output.

15.6 Rights of Management to Examine Data Stored on the Board’s Systems
All data stored in the Board’s computer and communications systems are the property of the Board. To properly maintain and manage these systems, the Board reserves the right to examine all data stored in or transmitted by these systems. Since the Board's computer and communication systems are used for business purposes only, staff are required to have no expectation of privacy associated with the information they store in or send through these systems.

15.7 Copying, Transferring, or Disclosing Software Prohibited
Staff members are not allowed to copy software provided by the Board to any storage media, transfer such software to another computer, or disclose such software to outside parties without appropriate authorisation. The Board strongly

supports strict adherence to software vendors' license agreements and copyright holders' notices. If any staff make unauthorised copies of software, they do so on their own behalf. All such copying is strictly forbidden by the Board.

15.8 Transfer of the Board's Information to Third Parties
The Board's software, documentation, and all other types of internal information is not to be sold or otherwise transferred to any non-Board party for any purposes other than business purposes expressly authorised by the Board.

15.9 Periodic Review of Software Licensing Agreements
The agreements for all computer programs licensed from third parties is reviewed regularly for the Board's compliance.

16.10 Security Incident Handling
The Secretary is to report any security incident to the Chairman of the Audit and Risk Committee. Refer to the Disaster Recovery Plan for information in the event of a disaster.

16.11 Compliance
It is the responsibility of all staff to be mindful of information security on a day-to-day basis.

17. Who Must Comply With Information Security Requirements
External consultants, contractors, and temporary staff are subject to the same information security requirements, and have the same information security responsibilities, as the Board's employees.

18. Disciplinary Measures for Information Security Non-Compliance
Non-compliance with the Computing Security Policy and associated, procedures is grounds for disciplinary action and may include termination of employment.

Further information

For further information concerning the Board's Computing Security Policy, please contact:

The Secretary
The Rice Marketing Board for the State of New South Wales
PO Box 151
LEETON NSW 2705

Telephone: (02 6953 3200
Facsimile (02) 6953 7684

E-mail: secretary@rmbnsw.org.au