THE RICE MARKETING BOARD FOR THE STATE OF NEW SOUTH WALES

Information Management Policy

Version	Author	Date Approved by Board
2009-1	Gillian Kirkup	24 March 2010
2017	Carol Chiswell	12 May 2017
2018-1	Carol Chiswell	16 October 2018
2019-1	Rose Kay	18 June 2019

THE RICE MARKETING BOARD FOR THE STATE OF NEW SOUTH WALES

INFORMATION MANAGEMENT POLICY

1 Purpose

This document describes the Information Management Policy of the Rice Marketing Board for the State of NSW (the Board). This policy establishes guidelines and responsibilities to protect the computing resources and records of the Board. The Board needs accurate, timely, relevant and properly protected information to operate effectively.

This policy ensures that full and accurate records of all activities, decisions and transactions of the Board are created and managed to meet the Board's business needs and accountability requirements. . The policy provides a framework and outlines responsibilities for the operation of Records Management and Computing Resources.

The establishment of a corporate Records Management Program is a requirement under section 12.2 of the *State Records Act 1998* (NSW). The Act provides that each public office must ensure the safe custody and proper preservation of the state's records that it has control of.

2 Scope

This Policy applies to all Board employees, Board members, contractors, consultants and temporary workers employed by the Board, including those workers affiliated with third parties, who access the Board's computer networks and records.

This Policy applies to all security measures relating to computer resources, records and archives including all types of media and systems. It covers all computing environments including desktop, laptop, network, remote access, email and Internet.

The Board Secretary provides individuals with access to the Board's systems where appropriate for authorised use only.

3 Definitions

Authorised use	Any use that is for the legitimate purpose of the Board.
Computer resources	Computer hardware, software, data, electronic

	information systems and networks, including the Internet, World Wide Web and email and devices and systems used to process and maintain information.
Electronic Communications	Communication using computer based tools that facilitate primarily non face to face communications. E.g. Email, Desktop Faxing, SMS, Video Conferencing, Messaging and Social Media.
Unauthorised use	Any use that is not for the legitimate purpose of the Board.
User	Anyone authorised to use the Board's computing environment including Board employees, Board members, contractors, consultants and temporary workers.
Hardware	The physical components of a computer or other electronic system.
Software	Applications and Programs used by computer systems.
Records Management Program	A co-ordinated set of policies, procedures and activities that are required to manage the records of the Board.
Access Control	Security techniques that regulate who or what can view or use resources in a computing environment. This includes physical such as buildings and rooms and logical such as computer networks, system files and data.
Centralised Records Management System	One central records management system that is used by all staff of the Board.
Information Management	Collection and management of the Board's Information from one or more sources and the distribution of that information.
Records	A piece of evidence about the past, especially an account kept in writing or in an electronic form. It is a document that memorises and provides evidence of activities performed, events occurred, results achieved or statements made. This can be in physical or media form. Records are evidence of activities for example Banking Records such as bank and credit card statements.
Data	Facts, figures or information stored in or used by a computer, for example an email or research paper.

4 Computing Policy

4.1 Use of computing resources

- The Board's computing resources are for authorised use only.
- Computing resources and records are to be properly protected from threats.
- When access is required to the Board's network from outside the office, the Board's official Virtual Private Network (VPN) is used. VPN is to be used for business purposes only.
- All data stored in the Board's computing resources 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.
- Users must practise good judgment to avoid printing and storage of unnecessary files and emails.

4.2 Software and Hardware

- All software and hardware purchases must be approved by the Board.
- Computer software and hardware purchases must not be connected to the Board's network unless they are compliant with software licensing obligations and contain the appropriate level of protection programs.
- Software must not be duplicated without the approval of the Board, and by agreement with the licenser.
- The Secretary is responsible for maintaining user logins and passwords for all computing resources including BoardEffect software and banking systems.
- Users are responsible for the security of their assigned devices, for example, the security of a laptop when travelling.
- An Uninterrupted Power Supply (UPS) unit is to be used to safeguard the electrical supply to all computing resources.
- Virus protection and firewalls are to be employed to protect against cyber threats.
- The server is to be located in a locked office only accessible to authorised personnel.
- The server is to be backed up daily and the Secretary is responsible for replacing back-up tapes once a week. Back-up tapes are to be kept in the Board's safe, except for one tape per month to be kept off-site and replaced monthly.
- The server is to be re-booted at least once a month.
- A Disaster Recovery Plan is to be maintained by the Board.
- The disposal of any computing equipment is to be approved by the Board.
- Data on computer equipment to be sold or otherwise disposed of must be destroyed or concealed prior to disposal.

4.3 Confidentiality of data

- All users have a responsibility to employ available security mechanisms and procedures for protecting corporate data.
- The Board's Secretary is responsible for making every endeavour, via both automated and manual processes, to protect the confidentiality and integrity of the Board's computing resources.
- Information held by the Board must not be accessed for unauthorised use.
- All information within the BoardEffect software is confidential and must not be shown or otherwise provided to anyone who is not a Board member or employee.
- 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 to be approved by the Board.
- Screensavers are to be automatically invoked after a fixed period of ten minutes.
- Board Members are obliged to ensure their computer systems are updated regularly to maintain virus protection and ensure the Board's information on their systems is not accessible to others.

4.4 Unauthorised use

- Use of the Board's computer systems for private financial gain is prohibited.
- Outbound electronic communications must not be inflammatory, harassing, defamatory, offensive, disruptive to other's operations, or otherwise reflect poorly on the reputation or image of the Board.
- It is prohibited for users to download, upload, copy, distribute or view any form of pornographic, racist or discriminatory content; any content that pertains to any form of criminal activity; and/or any content which may be considered by reasonable persons as offensive. This includes but is not limited to websites, email and any form of removable media.
- Employees must not 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.
- Users must not load or play computer games on the Board's computing resources.
- Users must not propagate chain letters, virus hoax emails, joke emails, documents or images.
- Users must have no expectation of privacy for any electronic communications or use of the Board's computing resources. Employees' use of computing resources may be monitored in accordance with the *Workplace Surveillance Act 2005 (NSW)*.

4.5 Access control

- Users must only log on under their own user name. Passwords must not be shared and must not be included in any documentation.
- Access rights are controlled through the use of passwords to prevent unauthorised access.
- In the event that a Board member or employee resigns, retires or is terminated, all physical security access codes known by the staff member are to be deactivated or changed.

5 Records Management Policy

5.1 Records Management

The Board recognises that its records are valuable information resources that are necessary for the effective and accountable conduct of its business. The objectives for Records Management are that:

- The Board has the records it needs to support:
  - ✓ ongoing business activity,
  - ✓ customer services,
  - ✓ accountability requirements, and
  - ✓ the expectations of the general public.
- The records of the Board are managed as effectively as possible, in order to best meet business needs
- The records of the Board are able to be easily retrieved when required, and
- The Board complies with all external requirements concerning its records and record management practices.

The Board's records management will be regularly reviewed against these objectives, to ensure it is meeting business needs.

5.2 Responsibilities for Records Management

Chair
The Chair of the Board is ultimately responsible for ensuring that the Board is compliant with its records management requirements and that it adequately manages the records necessary to sustain its business operations.

Corporate Records Manager
As the Board is a small statutory body, the Board Secretary will assume the role of Corporate Records Manager.

As Corporate Records Manager, the Secretary will be responsible for the development of recordkeeping procedures, training of staff and monitoring and analysis of Records Management. The Corporate Records Manager will also have overall responsibility for records management operations.

All RMB staff, including consultants and contractors
All staff are responsible for making and keeping adequate records of their business activities. This includes making records in situations where they otherwise would not be created, such as making records of meetings, phone conversations and verbal decisions.

Staff have a responsibility for ensuring that all records are adequately managed, according to the Board's procedures, and accessible where appropriate as corporate information resources to other Board staff. All staff should also be aware of the following records management rules:

- Records must be stored efficiently, to enable their accessibility and safety, to protect them against damage,
- Records must only be destroyed when authorised under the *State Records Act 1998* (NSW), and

Records must be stored securely to maintain the confidentiality of information, having regard to the Board's Privacy Policy and Codes of Conduct.

5.3 Electronic records

Electronic records are stored on the Board's server and on external hard-drives that are backed-up regularly.

5.4 Administrative setting of the Records Management Program

As the Board is a small organisation with a small number of staff working in the same location, it has adopted a centralised records management structure. This means there is one central records management system that is used by all staff of the Board.

5.5 Legislative requirements for recordkeeping

The following legislation and best practice requirements affect or govern the Board's records management program:

- State Records Act 1998
- Government Information (Public Access) Act 2009
- Privacy and Protection of Personal Information Act 1998
- Evidence Act 1995
- Public Finance and Audit Act 1983
- Public Authorities (Financial Arrangements) Act 1987

- NSW Treasurer's Guidelines
- NSW Ombudsman's Good conduct and administrative practice: guidelines for public authorities and officials
- Australian Standard AS ISO 15489 on Records Management

5.6 Planning and monitoring

This policy will also be reviewed at regular intervals to ensure it continues to reflect best practice and the Board's business needs.

5.7 Periods of Retention

It is the policy of the Board to retain the following records indefinitely: Board minutes, assets register, land ownership records, annual audited financial statements and annual reports.

It is the policy of the Board to retain the following records for twenty years: Capital Equity Rollover Scheme contribution details.

It is the policy of the Board to retain the following records relating to the Capital Equity Rollover Scheme, for seven years: certificates, applications for redemption, statutory declarations, rollover payment details and grower correspondence.

It is the policy of the Board to retain the following general records for seven years: Accounts receivable and accounts payable invoices and receipts, financial management reports, finance facility and investment documents, crop audit and export audit documents and general correspondence.

5.8 Historic documents

Documents that are deemed by the Board to be historic documents are to be stored in accordance with best practice conservation methods and comply with the NSW State Records Act 1998.

6 Consequences

Non-adherence to this Policy may result in disciplinary action which may include termination of employment. Individuals may be prosecuted to the full extent of the law for unauthorised use of the Board's computing resources and records.

7 Communication

In order that all 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 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 if required.
- The Policy is published on the Board's website: www.rmbnsw.org.au.

8 Further information

For further information concerning the Board's Information Management 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

8.1 Document Approval and Control

a. Version

Reference	Details
File Name	Information Management Policy
File location	Z:/RMB Policies
Version	2019-1
Status	FINAL

b. Revision History

Version	Revision Date	Summary of Change	Author
2018.1	Sept 2018	Audit and Risk Committee	C Chiswell
2019-1	May 2019	Amalgamate Computing and Records Management Policies	R Kay

c. Document Approval

Board Approval	12/5/17
Audit and Risk Committee	21/5/19
Board Approval	18/6/19