THE RICE MARKETING BOARD FOR THE STATE OF NEW SOUTH WALES

Cyber Security Policy

THE RICE MARKETING BOARD FOR THE STATE OF NEW SOUTH WALES

CYBER SECURITY POLICY

1 Purpose

This document describes the Cyber Security Policy of the Rice Marketing Board for the State of NSW (the Board). It aims to align the Board's approach to cyber security with that of the NSW Cyber Security Strategy.

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.

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

3 Policy Statement

The Board recognises its obligations to protect the confidentiality, integrity and availability of the assets within its custody. It is committed to ensuring effective cyber security to safeguard the information of the Board and our stakeholders.

The Board has a risk-based approach to cyber security.

4 Responsibilities

The Board Secretary, with oversight by the Audit and Risk Committee, is responsible for management of cyber security risks and implementation of appropriate controls. The Audit and Risk Committee acts as the Information Security Steering Committee and is responsible for ensuring the Board's on-going commitment to cyber security principles and practice.

The Board is required to monitor and report on the effectiveness and relevance of its information security management system by:

- reporting annually to the Chief Information Security Officer of the Department of Planning, Industry and Environment;
- identifying cyber security risks with a residual rating of high or extreme and report these to Cyber Security NSW;
- confirming all data is secure; and
- attesting to cyber security in the Board's Annual Report.

5 Framework

The Board's cyber security is implemented according to the following approach:

- all information assets are identified and assessed for 'crown jewels' status and threat risk level. This includes non-Board devices and access from a non-Board location;
- all employees undertake annual training in cyber security;
- an incident response plan is available and will be implemented if a significant breach occurs; and
- when the Board regularly shares data with other entities, the data is classified and appropriate Agreements are in place.

6 Managed Service Provider

The Board uses a Managed Service Provider to handle its computer needs. The Managed Service Provider agrees to:

- subscribe to, and be aware of, the NSW Cyber Security Guidelines;
- align with the Board's specific information security management system requirements; and
- provide specialist cyber security information and training on request.

7 Definitions

Asset	Operational systems or information that has value to the Board
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.
Crown jewels	The Board's most valuable or operationally vital systems or information.
Cyber event	Has the potential to become a cyber incident and includes (but not limited to) multiple sequential failed logins for a user, inappropriate deletion or modification to system files or unauthorised access.
Cyber incident	A breach of this policy that requires corrective action. Examples are virus or malware attacks, denial of service attacks that affect system availability, compromise of sensitive or personal information or compromise of email account.
Electronic	Communication using computer based tools that

Communications	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.

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

9 Document Approval and Control

a. Version

Reference	Details
File Name	Cyber Security Policy
File location	Z:/RMB Policies
Version	2021-1
Status	FINAL

b. Revision History

Version	Revision Date	Summary of Change	Author
2021.1	28/9/21	Creation	C Chiswell

c. Document Approval

Board	21/10/21