Cybersecurity Management Plan

Rural Funds Management
ABN 65 077 492 838
AFSL 226701

Effective date: 27 January 2026	**Reviewed:** Annually
Owner: National Manager – People and Safety	**Approval:** Board

Policy

Rural Funds Management (**RFM**) recognises the risk of data theft, scams, and security breaches and the impact it can have on systems, technology infrastructure, and reputation. This management plan outlines the security measures to ensure business data remains secure and protected and how RFM will recover from an incident.

Purpose

This Plan addresses:

Cybersecurity – the tools, processes, and procedures in place to prevent a cyber incident.

Cyber resilience – how RFM will react after a cyber incident.

Scope

This Plan applies to all RFM and all entities which are owned and/or managed by RFM and their employees.

Internal references

- ICT Infrastructure
- ICT Policy and Procedures
- Risk Management Policy

External references

- https://www.cyber.gov.au/
- http://www.auscert.org.au
- http://www.staysmartonline.gov.au
- http://www.scamwatch.gov.au
- https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls
- ASIC Regulatory Guide 259

Need help?

Any queries regarding this Plan should be directed to the ICT team (IT@ruralfunds.com.au).

Introduction

1. Information and communication technology (**ICT**) systems and information are constantly challenged by evolving hardware, software, threats and regulations. Effective protection of business information creates a competitive advantage. This is achieved by preserving data and by reducing the risk of incidents. RFM acknowledges the risk to its data through cybercrime and strives to protect its data through the implementation of cybersecurity measures.

Mitigation strategies

2. RFM has implemented mitigation strategies incorporating the *Essential Eight Strategies to Mitigate Cyber Security Incidents,* as published by the Australian Cyber Security Centre, as well as other strategies to be cyber resilient in response to threats. RFM aims to meet the strategies outlined at level two. This Plan does not guarantee protection against all cybersecurity threats but rather, demonstrates that cybersecurity risks and measures are being identified and managed in a way that is appropriate for the information value, the business environment and objectives of the business. There are many cybersecurity approaches that can secure networks. These *essential eight mitigation strategies* have been developed to provide baseline details to protect networks, users, applications and data.

Essential Eight Maturity Model – Maturity Level 2

The focus of this maturity level is adversaries operating with a modest step-up in capability form the previous maturity level. These adversaries are willing to invest more time in a target and, perhaps more importantly, in the effectiveness of their tools. For example, these adversaries will likely employ well-known tradecraft to better attempt to bypass security controls implemented by a target and evade detection. This includes actively targeting credentials using phishing and employing technical and social engineering techniques to circumvent weak multi-factor authentication.

Generally, adversaries are likely to be more selective in their targeting but still somewhat conservative in the time, money and effort they may invest in a target. Adversaries will likely invest time to ensure their phishing is effective and employ common social engineering techniques to trick users to weaken the security of a system and launch malicious applications, for example via Microsoft Office macros. If the account that an adversary compromise has special privileges, they will seek to exploit it, otherwise they will seek accounts with special privileges. Depending on their intent, adversaries may also destroy all data (including backups) accessible to an account with special privileges.

3. Prevent

Strategy	Function	Why
Control	Restricts access to trusted applications to prevent executing malicious code or scripts	All non-approved applications (including malicious code) are prevented from executing.
Updating and patching	Updates applications to remedy previously unidentified vulnerabilities (exploits)	Security vulnerabilities in applications or operating systems can be used to execute malicious code.

Application hardening	Blocks or restricts access to potentially harmful online applications	Prevent malware from entering the corporate network.

4. Limiting

Strategy	Function	Why
Restrictions	Allows only trusted users to manage systems, install software and apply patches	Unauthorised users and intruders from carrying out malicious activities.
Multi-factor authentication	Most effective controls to prevent an adversary from gaining access to a device or network	Stronger user authentication makes it harder for adversaries to access sensitive information and systems.
Disabling or limiting	Disabling macros or embedded codes	Macro-borne malware from entering the corporate network.

5. Recovery

Strategy	Function	Why
Backup	Allows only trusted users to manage systems, install software and apply patches	To ensure information can be accessed following a cybersecurity incident (e.g. a ransomware incident).
Recovery	Plan to implement data recovery process and responsibility in a case of a security incident	To ensure correct procedures are followed.

6. Other strategies

- Security consultation with third party specialists and consultants as required.
- Monitoring alongside a number of collaborators such as ACSC and ACCC, to help growth, adaptability, advice, solutions and to draw on collective understanding, experience, skills and capability to lift cyber resilience.
- Adopt security bulletins to receive up to date and consistent security bulletins across a wide range of vendors, streamlining security patching.
- Training and education, security awareness training for employees. Education and training may be delivered formally through training sessions, educational emails and guides or external courses. Informal education and training are provided to individual users on an as needs basis, in conjunction with ICT support.
- Implementation of cryptographic and security protocols techniques.
- Streamlining an effective business continuity and disaster recovery plan.
- Ensuring responsible and ethical use of AI tools.

7. Responsibilities

Role	Responsibilities
All Managers	• Promoting an information security culture.
Compliance team	• Monitoring compliance with this Plan • Advising the ICT team of compliance changes • Promoting an information security culture.
National Manager – People and Safety	• Reporting to the Board on ICT strategy, programs and plans and incidents • Approving cybersecurity audits, reviewing results and deciding on corrective actions • Promoting an information security culture.
ICT Project Coordinator	• Liaising with external IT provider re ICT systems coordination, implementation, monitoring, administration and support • Liaising with external IT provider for advice on ICT (including cybersecurity) strategy, establishing programs and plans, including: o Security awareness o Risk management o Response and recovery • Participating in cybersecurity audits and reviewing recommendations • Delivering cybersecurity education and advice.
Asset Owners	• Managing the administration, security and integrity of an application or software used at RFM • Ensuring any application or software used is appropriately secured, documented (particularly in relation to the coding language used), tested for vulnerabilities and source code is retained • Ensure that third party agreements address information security and privacy • Ensuring cybersecurity threats are managed in accordance with this Plan.
All Employees	• Ensuring passwords are protected from loss or disclosure • Ensuring RFM assets are protected from loss • Reviewing and discussing cybersecurity requirements prior to the introduction of any new or updated systems and applications • Reporting any known weaknesses to the ICT team • Complying with the requirements of this Plan and the ICT Policy

Role	Responsibilities
	• Reporting incidents to the ICT team as soon as they are recognised and electronically reporting them to the incident management system • Participating in education and training.

Reporting Cybersecurity incidents

8. An ICT incident is considered a security threat. It includes incidents that compromise or could compromise the confidentiality or integrity of information held. Examples of cybersecurity incidents include:

    - Unauthorised access
    - System intrusion and virus outbreaks
    - Suspicious, inappropriate or offensive email
    - Theft of hardware, documents, storage media, etc
    - Personal, confidential or inside information made publicly available through inappropriate use of AI systems.

9. All security incidents and security weaknesses that may affect RFM or compromise information and systems, must be reported to the ICT team (IT@ruraflunds.com.au) as soon as it is known. RFM ICT Team will report substantiated incidents to the online incident reporting system.

Cyber resilience

10. Cyber resilience refers to how we react to a cyber threat and/or incidents. As an AFSL holder, RFM endeavours to follow ASIC's good practice guide[1] ensuring a responsive cyber resilience process exists within the organisation.

    RFM has put the following in place to increase its cyber resilience:

    - Implementation of the RFM Business Continuity and Disaster Recovery Plan
    - Established an insurance policy covering losses and costs associated with cyber threats and/or incidents
    - Data backup and recovery procedure
    - Utilisation of external consultants and specialists to facilitate investigations and expedient recovery of data.

11. Furthermore, RFM ensures the Board is kept abreast of any IT issues:

    - Receiving monthly compliance reports[2]
    - Regular IT testing and training is performed[3]

[1] Cyber resilience good practices | ASIC

[2] Data Breach Policy paragraph 17, RFT Master Compliance Plan

[3] RFT Master Compliance Plan

- Monitoring of external service providers[4]
- Regular review of material IT risks.[5]

Definitions

Acceptable Use	Behaviours and actions, in connection with the use of RFM ICT Services, which are permitted under the ICT Acceptable Use Policy
Accountable Officer	Accountable employees within RFM
AFSL	Australian Financial Services Licence. RFM's AFSL is 226701
Asset Owner	An individual or group with accountability and authority for a specific application or software used at RFM.
Authorised User	A person who has been granted access
Authentication Credential	Username/passcode, PIN or other secret keys used to gain access to ICT services
Capability	The capacity an organisation needs to perform a business function
Control	A measure put in place to eliminate or minimise risk
Cyber resilience	How we react after an incident
Cybersecurity	The tools, processes and procedures in place to prevent a cyber incident
Information Security	The protection and preservation of information
ICT Services	Services provided to an Authorised User including software, communication devices, and computing infrastructure under the control of the RFM or a third-party provider on behalf of RFM
RFM	Rural Funds Management Limited (ACN 077 492 838), and includes its subsidiary companies and any entity for which it is responsible entity

[4] RFT Master Compliance Plan
[5] Risk Management Policy