Policy P5.1.3
Information Security Management

Version	2.1
SOPs	SOP P5.1.3-1 Responsibilities SOP P5.1.3-2 Information Security Management
Policy Owner	Executive Director Technology, Finance & Legal
Policy Contact	Director ICT/Chief Information Officer
Approval Date	8 October 2024
Next Review	8 October 2025

1 Purpose

1.1 The RFS recognises that Information and Communications Technology (ICT) systems and information are assets that, like other important assets, are essential to its business and consequently need to be suitably protected.

1.2 The RFS is committed to maintaining appropriate levels of security, protecting all systems and ICT assets from a wide range of threats, ensuring business continuity, minimising business risk, and maximising return on investments and effective business support.

1.3 This policy applies to all:

- ICT systems managed and controlled by the RFS, and all users of ICT systems;
- users of RFS ICT systems including RFS members, temporary staff, visitors, external agency, contracted users and other third parties;
- sections of the RFS and its service providers for information assets that contain:
  - identifiable information about members of the public; and
  - sensitive identifiable information about staff or contractors, classified and DLM marked under NSW Government Information Classification and Labelling Guidelines.

1.4 This policy articulates the mandatory security controls to be applied by all users of ICT across the RFS, and complies with the requirements of Service Standard 1.1.14 Personal Information and Privacy.

2 Policy

Information Security Management

2.1 The RFS Information Security Management System (ISMS) outlines the strategic direction and aligns with the NSW Cyber Security Policy (CSP) which broadly incorporates elements of ISO27001 Cybersecurity, National Institute of Standards and Technology - Cybersecurity

Framework (CSF), ISO27001 Cybersecurity and the Australian Signals Directorate – Information Security Manual.

2.2 The overall objective of the RFS ISMS is to ensure that the confidentiality, integrity and availability of ICT systems, information assets, related ICT and IACS infrastructure are preserved in a consistent and risk-considered manner which best suits the strategies, objectives and needs of the RFS.

2.3 The ISMS framework will be applied consistently across the RFS.

2.4 The RFS adopts a risk management approach to defining, maintaining and continually improving the ISMS. The risk assessment performed in the ISMS will be in accordance with P7.1.10 Enterprise Risk Management and related Framework.

2.5 The ISMS will ensure contracts and agreements with key service providers define explicit obligations and responsibilities relating to information and system security.

2.6 The ISMS will ensure all staff, volunteers, service providers, contractors and visitors are aware of their information security responsibilities and that they are appropriately trained to meet those responsibilities. SOP P5.1.1-1 Responsibilities provides detail on the responsibilities of various roles.

Review

2.7 This policy will be reviewed annually by the end of the financial year, in line with the Digital NSW Cyber Security Policy requirements.

3 Definitions

3.1 For the purpose of this policy document the following definitions and acronyms apply:

- **Cyber Security:** the preservation of confidentiality, integrity, and availability of information in the cyberspace.
- **Cyberspace:** a complex environment resulting from the interaction of people, software, and services on the internet by means of technology devices and networks connected to it.
- **Cyber Security Policy (CSP)**: The policy that provides information on the measures used to protect the confidentiality, integrity and availability of systems, devices, and the information residing on them
- **Information Security Management System (ISMS):** the policies, procedures, guidelines and associated resources and activities that the RFS has implemented to protect its information assets. It is a systematic risk-based approach to establishing, implementing, operating, monitoring, reviewing, maintaining and improving our information security.

4 Document control

Release history

Version	Date	Summary of changes
1.0	14 December 2009	Initial release
	1 June 2016	Policy repealed and content updated and incorporated into P5.1.1 ICT Equipment Standards and Security v2.0
2.0	17 May 2019	Reinstated – ICT security needs to be covered by a stand-alone policy to align with current regulatory requirements – NSW

Version	Date	Summary of changes
		Cyber Security Policy, DFSI Information Security policy and ISO 27001 Cybersecurity Change of title from “ICT Security” to “Information Security Management”
2.1	8 October 2024	Scheduled review and minor amendments to reflect current obligations and practice.

Approved by

Name	Position	Date
Rob Rogers AFSM	Commissioner	8 October 2024

Related documents

Document name
NSW Government ICT Assurance Framework
NSW Government Information Management Framework
NSW Government Procurement Policy Framework
NSW Treasury Circular TPG22-12 NSW Gateway Policy
NSW Government Open Data Policy
NSW Government Data Policy
NSW Cyber Security Policy
ISO 27001 Cyber Security
ASD Information Security Manual
National Institute of Standards and Technology - Cybersecurity Framework (CSF)
Service Standard 1.1.14 Personal Information and Privacy
Service Standard 1.4.4 Volunteer and Visitor Access to Network Services and Data
Service Standard 5.1.3 Communication Systems
Policy P4.1.9 Communications – Mobile and Data Devices
Policy P4.1.3 Procurement
Policy P5.1.2 Acceptable Use of Information and Communication Technology (ICT)
Policy P5.1.6 Records Management
Policy P7.1.10 Enterprise Risk Management
RFS ICT Standards and Procedures

SOP P5.1.3-1
Responsibilities

1 Purpose

1.1 This Standard Operating Procedure (SOP) provides details on the responsibilities of various roles in the management of Information Security Management.

2 Procedures

2.1 Responsibilities of various information security management roles are shown in the table below:

Role	Responsibilities
RFS Commissioner	– attests on cyber security in the RFS Annual Report and provides a copy to NSW Government Chief Information Security Officer (GCISO). – Approves publication of this policy.
Chief Information Officer (CIO)	– recommends endorsement of this Policy to EDTFL for Commissioner approval.
Chief Information Security Officer (CISO)	– review and update the ISMS Policy and ISMS Procedure annually, or sooner if required, manage the overall development, implementation, maintenance, review and continual improvement of the ISMS across the RFS. – coordinate the review and update of the Threat and Risk Assessment, Risk Treatment Plans, Statement of Applicability and documented controls and procedures. – coordinate internal ISMS audits and ensure that corrective and preventive actions are applied as required. – ensure the ISMS continues to conform with the requirements of the NSW Cyber Security Policy, RFS Information Security Management Policy, RFS Enterprise Risk Management Framework and other relevant authorities. – measure and report on the performance of the ISMS to the ICT Governance Group and the Audit & Risk Committee.
ICT Cybersecurity Governance Group	– approve necessary resources to establish, implement, operate, monitor, review, maintain and improve the RFS' ISMS. – conduct a Management Review of the ISMS at least annually and ensure that corrective and preventive actions are applied as required. – advocate, promote and demonstrate its ongoing commitment to the ISMS and the continual improvement of information security across the RFS.
RFS ICT Managers	– participate in the ISMS Threat and Risk Assessment process and ensure that threats and risks within the register remain up to date. – participate and co-operate with ISMS Internal Audits. – ensure that corrective and preventive actions are applied by due dates.

Role	Responsibilities
	– ensure that risk treatments in the ISMS Risk Treatment Plans are actioned by the due dates. – ensure security responsibilities and expectations are clearly defined in service provider contracts and agreements and that those responsibilities are monitored. – ensure that staff, contractors and service providers who have a role to play in the ISMS are trained and remain competent to fulfil their duties.
RFS permanent and temporary staff, visitors, external agency, and contracted users and other third parties;	– comply with all RFS policies and service standards including the P5.1.2 Acceptable Use of Information Communication and Technology policy. – participate in information security training. – remain aware of their information security roles and responsibilities.

SOP P5.1.3-2
Information Security Management

1 Purpose

1.1 This Standard Operating Procedure (SOP) details the requirements of the Information Security Management policy statements.

2 Procedures

2.1 The information security management system (ISMS) is a set of standards, procedures and associated controls designed to manage RFS information systems, ensuring compliance with the requirements of the RFS Information Security Management Policy

2.2 The ISMS will be reviewed and updated by the Chief Information Security Officer annually or as updates are required and approved by the Security Risk & Compliance Board.

ISMS Threat and Risk Assessment

2.3 Risk assessments will be performed in accordance with Policy P7.1.10 Enterprise Risk Management and related Framework.

2.4 Threats that can impact the confidentiality, integrity or availability of the 'in scope' assets of the RFS will be identified, registered and assigned to the risk owner, along with the impact and likelihood of those threats.

2.5 Risks will be quantified and documented as part of an ISMS Threat and Risk Assessment. The risks that breach RFS risk appetites are reported to the Audit and Risk Committee and other relevant RFS executive and governance groups.

2.6 The Threat and Risk Assessment will be reviewed and updated by the Chief Information Security Officer annually or sooner if required.

ISMS Risk Treatment Plan

2.7 An ISMS Risk Treatment Plan will be documented, implemented and maintained for each instance where current risk exceeds acceptable risk (as identified by the Threat and Risk Assessment), to ensure that the confidentiality, integrity and availability of information assets are maintained within acceptable levels.

2.8 The Risk Treatment Plan will be reviewed and updated by the Security Risk & Compliance Board annually or sooner if required.

ISMS Statement of Applicability

2.9 An ISMS Statement of Applicability will be documented, implemented and maintained, which specifies the applicability of each control and control objective listed along with a justification for the inclusion or exclusion of each.

2.10 The Statement of Applicability will be reviewed and updated by the Security Risk & Compliance Board and approved by CIO and EDTFL annually or sooner if required.

ISMS Controls and Procedures

2.11 ISMS controls are designed to address risks to information security. Controls come with Standards and Procedures to achieve Information Security Policy objective. Below is the list of ISMS controls that must be taken into account:

- Information Security Awareness
- Identity and Access Control

- Data Classification and Information Handling
- Vulnerability & Patch Management
- Supply Chain and Third-Party Management
- Security Logging and Monitoring
- Network Security
- Email and Communication
- Cybersecurity Incident Management
- Remote Work
- Bring Your Own Device
- Mobile Security
- Physical Security
- Password and Credential Management
- Cryptography and Key Management
- Security Configuration Management
- Endpoint Security
- Cloud Security
- Secure SDLC and IaC
- Application Security
- Human Resource
- API Security
- OT Security
- AI Security
- Container Security
- Kubernetes Security
- Serverless Security
- Open-Source Security

2.12 A documented standard, and procedures will be maintained for each selected control as noted within the Statement of Applicability.

2.13 Each documented standard and related procedure will specify the way the control is to be applied and how the effectiveness of the control (or group of controls) is to be measured.

2.14 The SRCB conducts regular reviews of the ISMS controls compliance to maintain the effectiveness of the information security management system.

Control of Documents and Records

2.15 All ISMS documents and associated records will be maintained and stored in a controlled manner in accordance with specifications defined within the ISMS Procedures, in addition to the requirements of Policy P5.1.6 Records Management.

Management Commitment

2.16 The RFS ICT Cybersecurity Governance Group will provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS as defined in the ISMS Procedure.

Provision of Resources

2.17 The CISO will provide necessary resources to establish, implement, operate, monitor, review, maintain and improve the RFS ISMS as defined in the ISMS Procedure.

Training, Awareness and Competence

2.18 All staff and contractors who are assigned responsibilities within the ISMS Procedure will undertake ongoing training to ensure they remain aware of those responsibilities and competency to perform those tasks.

Internal ISMS Audits

2.19 ISMS Internal Audits will be conducted at planned intervals to determine whether ISMS control objectives, controls, processes and procedures are functioning in an effective manner and whether staff, contractors and service providers are complying with the controls and procedures set out in this policy and ISMS Procedure.

2.20 Results of ISMS Internal Audits will be reported to the Security Risk & Compliance Board and the Audit and Risk Committee.

Management Review of ISMS

2.21 The Security Risk & Compliance Board will conduct a management review of the ISMS at least annually as defined in the ISMS Procedure to ensure its suitability, adequacy and effectiveness.

Continual Improvement

2.22 The RFS will continually improve the effectiveness of its information security capabilities, and its ISMS as a whole, through the application of this policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions, and management review as defined in the ISMS Procedure.