NSW GOVERNMENT

NSW RURAL FIRE SERVICE

POLICY P5.1.3
INFORMATION SECURITY MANAGEMENT

ITEM	DESCRIPTION
Version Number	2.0
SOPs	› SOP P5.1.3-1 Responsibilities › SOP P5.1.3-2 Information Security Management
Owner	Executive Director, Infrastructure Services
Contact	Director, ICT and Chief Information Officer
Approved Date	17 May 2019
Effective Date	22 May 2019
Next Review Date	Annual review (to be completed by end of each financial year)
Document Control	Electronic - Printed Copies are Uncontrolled

1 Purpose

1.1 The NSW Rural Fire Service (NSW RFS) recognises that Information and Communication 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 NSW 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:

a. covers all ICT systems managed and controlled by the NSW RFS, and all users of ICT systems;

b. covers all Industrial Automation and Control Systems (IACS) managed and controlled by the ICT section, and all users of IACS systems;

c. applies to all NSW RFS members, external agency and contracted users;

d. applies to all sections of the NSW RFS and its service providers for information assets that contain:

i. identifiable information about members of the public; and

ii. sensitive identifiable information about staff or contractors, classified and DLM marked under NSW Government Information Classification and Labelling Guidelines; and

e. articulates the mandatory security controls to be applied by all users of ICT across the NSW RFS.

2 Definitions

2.1 For the purpose of this Policy Document, the following definitions and acronyms apply:

a. **Cyber Security:** the preservation of confidentiality, integrity and availability of information in the cyberspace.

b. **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.

c. **CSP:** Cyber Security Policy.

d. **ISMS:** Information Security Management System

e. **Industrial Automation and Control System (IACS)**: includes systems such as video surveillance, alarms, personnel safety and building management systems.

3 Policy

Information Security Management

3.1 The NSW RFS ISMS outlines the strategic direction in line with NSW Cyber Security Policy (CSP).

3.2 The ISMS will comply with the requirements of the NSW CSP and the Department of Finance, Services and Innovation (DFSI) Information Security Policy which is broadly aligned with ISO 27001 'Information Security Management System'.

3.3 The overall objective of the NSW 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 NSW RFS.

3.4 The ISMS framework will be applied consistently across the NSW RFS.

3.5 The NSW RFS adopts a risk management approach to defining, maintaining and continually improving the ISMS. The risk assessment performed in the ISMS will align with P7.1.10 Organisational Risk Management and related Framework.

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

3.7 The ISMS will ensure all staff, volunteers, service providers and contractors 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

3.8 This policy will be reviewed annually by the end of the financial year, in line with the DFSI Cyber Security Policy reporting requirements.

4 Related documents

- *Privacy and Personal Information Protection Act 1998*
- *Copyright Act 1968*
- NSW Government ICT Assurance Framework
- NSW Government Information Management Framework
- NSW Government Procurement Policy Framework
- NSW Treasury Circular 10/13 Gateway Review System
- NSW Department of Premier and Cabinet Circular C2005-06 Intellectual Property Management Framework the NSW Public Sector.
- NSW Government Open Data Policy
- NSW Government Data Information and Custodianship Policy
- NSW Cyber Security Policy
- ISO/IEC 27001 Information Security Management System
- Department of Finance and Services DP0036 v3.0 Acceptable Use Policy
- Service Standard 1.1.7 Code of Conduct and Ethics

- Service Standard 1.1.14 Personal Information and Privacy
- Service Standard 1.1.26 Volunteer and Visitor Access to Network Services and Data
- Service Standard 5.1.3 Communication Systems
- Policy 3.1.1 Communications
- Policy P4.1.3 Procurement
- Policy P5.1.2 Acceptable Use of Information and Communication Technology (ICT)
- Policy P5.1.6 Records Management
- Policy P5.1.7 ICT Disaster Recovery
- Policy P7.1.4 NSW RFS Corporate Planning and Reporting
- Policy P7.1.9 Business Continuity Management
- Policy P7.1.10 Organisational Risk Management
- NSW RFS Corporate Plan 2014-2021
- NSW RFS Enterprise Architecture
- NSW RFS ICT Strategic Plan
- NSW RFS Password Standards
- NSW RFS Data Security Standards
- NSW RFS Secure Software Development Standards
- NSW RFS Security Incident Response Plan

5 Amendments

AMENDMENT DATE	VERSION NO	DESCRIPTION
14 December 2009	1.0	› Initial release
1 June 2016	*Repealed*	› *Repealed - Content updated and incorporated into P5.1.1 ICT Equipment Standards and Security v2.0*
17 May 2019	2.0	› **Reinstated** - ICT security needs to be covered by a stand-alone policy to align with current regulatory requirements - NSW Cyber Security Policy, DFSI Information Security Policy and ISO 27001 Information Security Management System › Change of title from “ICT Security” to “Information Security Management”

SOP P5.1.3-1

Responsibilities

1 Purpose

1.1 This 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
NSW RFS Commissioner	➤ attest on cyber security in the NSW RFS annual reports and provide a copy to NSW Government Chief Information Security Officer (GCISO).
Chief Information Officer (CIO)	➤ recommends endorsement of this Policy to EDIS
ICT Governance Group	➤ approve necessary resources to establish, implement, operate, monitor, review, maintain and improve the NSW 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 NSW RFS.
Enterprise Architecture Working Group	➤ 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 NSW 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, NSW RFS Information Security Management Policy, NSW 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.
Information Security Officer	➤ act on behalf of the Enterprise Architecture Working Group in the development/adoption and enforcement of Information Security policies, procedures and standards for NSW RFS.
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
Managers (cont'd)	➤ 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.
Staff	➤ comply with all NSW 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

For more detail on the statements below refer to the ISMS Procedure.

ISMS Procedure

2.1 An ISMS Procedure will be documented and consistently applied, defining the processes and procedures to be followed in order to meet the policy statements and in order to satisfy the requirements of the NSW CSP broadly aligned to the ISO 27001 standard.

2.2 The ISMS Procedure will be reviewed and updated by the Information Security Officer annually or as updates are required and approved by the Enterprise Architecture Working Group.

ISMS Threat and Risk Assessment

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

2.4 Threats that can impact the confidentiality, integrity or availability of the 'in scope' assets of the NSW RFS will be identified, 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.

2.6 The Threat and Risk Assessment will be reviewed and updated by the 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 ICT Infrastructure & Security Architect 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 at Annex A of the ISO 27001 standard, along with a justification for the inclusion or exclusion of each.

2.10 The Statement of Applicability will be reviewed and updated by the ICT Infrastructure & Security Architect annually or sooner if required.

ISMS Controls and Procedures

2.11 A documented procedure will be maintained for each selected control as noted within the Statement of Applicability.

2.12 Each documented procedure will specify the manner in which the control is to be applied and how the effectiveness of the control (or group of controls) is to be measured.

2.13 The ICT Infrastructure & Security Architect will coordinate the review and update of these documented procedures annually or sooner if required.

Control of Documents and Records

2.14 All ISMS documents and associated records will be maintained and stored in a controlled manner in accordance with specifications defined within the ISMS Procedures and Policy P5.1.6 Records Management.

Management Commitment

2.15 The NSW RFS ICT 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

2.16 The ICT Director / CIO will provide necessary resources to establish, implement, operate, monitor, review, maintain and improve the NSW RFS' ISMS as defined in the ISMS Procedure.

Training, Awareness and Competence

2.17 All staff and contractors who are assigned responsibilities within the ISMS Procedure will be trained on an ongoing basis to ensure they remain aware of those responsibilities and that they remain competent to perform those tasks.

Internal ISMS Audits

2.18 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.

2.19 Results of ISMS Internal Audits will be reported to the NSW RFS ICT Governance Group, and the Audit and Risk Committee.

Management Review of ISMS

2.20 The ICT Governance Group will conduct a Management Review of the ISMS at least once a year as defined in the ISMS Procedure to ensure its suitability, adequacy and effectiveness.

Continual Improvement

2.21 NSW 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.

3 Related forms

- None