NSW RURAL FIRE SERVICE

POLICY P5.1.1
ICT EQUIPMENT STANDARDS AND SECURITY

ITEM	DESCRIPTION
Version Number	2.1
SOPs	› SOP P5.1.1-1 ICT Equipment Standards and Security
Owner	Executive Director, Infrastructure Service
Contact	Director, Information and Communications Technology (Chief Information Officer)
Approved Date	30 June 2017
Effective Date	30 June 2017
Next Review Date	30 June 2020
Document Control	Electronic - Printed Copies are Uncontrolled

1 Purpose

1.1 A higher degree of reliability, security, ease of use, economies of scale and improved service delivery results from the use of standardised Information Communication and Technology (ICT) hardware, software, communications and mobile equipment (ICT Equipment).

1.2 The NSW Rural Fire Service (NSW RFS) recognises that ICT systems are assets that, like other important assets, are essential to its business and consequently need to be suitably protected.

1.3 ICT security is defined as the preservation of confidentiality, integrity and availability of ICT assets, and involves the protection of ICT assets from a wide range of threats in order to ensure business continuity, minimise business risk, and maximise return on investments and effective business support.

1.4 This policy:

a. Covers standards for new, current and/or replacement hardware, software, communications and mobile equipment; and

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

1.5 All ICT procurement will be aligned with P4.1.3 Procurement Policy.

2 Policy

Equipment

2.1 The selection and procurement of new and replacement ICT equipment should comply with the Service's ICT standards (among others, the NSW RFS Enterprise Architecture, Government directives, and relevant legislation).

2.2 In some cases there is a genuine requirement for ICT equipment that does not comply with clause 2.1. For exceptions refer to SOP P5.1.1 – 1 ICT Equipment Standards and Security.

2.3 The procurement of all ICT equipment intended for use on the NSW RFS network should comply with NSW Government and NSW RFS standard replacement cycles and P4.1.3 Procurement policy.

2.4 For the life cycle of the product or service the person arranging procurement of new ICT equipment, software or services must ensure it is accompanied by a support agreement (for example, but not limited to, a warranty) provided by the vendor and/or recommended support representatives. If assistance is required refer to the Service Catalogue to arrange an ICT exception assessment service. New equipment, software or services without a minimum support agreement or exception in place, are not permitted on the NSW RFS network and will not be supported by the ICT Service Desk.

2.5 All computers used on the NSW RFS network must use the NSW RFS ICT developed standard operating environment (SOE) and associated licensed software. For exceptions, refer to SOP P5.1.1 – 1 ICT Equipment Standards and Security. Devices connected and used on the guest wireless network are excluded from this clause.

2.6 Non-standard software may be approved for use on the NSW RFS network by following the approved ICT Standards Exception process.

2.7 All ICT equipment will need to be replaced at the 'End of Life' period, i.e. four years for desktops and laptops, and three to five years for other ICT equipment.

ICT Security

2.8 The overall objective of ICT security within the NSW RFS is to ensure that the confidentiality, integrity and availability of ICT systems is preserved in a consistent and risk-considered manner which best suits the strategies, objectives and needs of the NSW RFS.

2.9 This policy covers all ICT systems managed and controlled by the ICT department, and all users of ICT systems. It applies to all full time, part-time, casual and contract staff, as well as all external agency users.

2.10 The NSW RFS adopts a risk management approach to defining, maintaining and continually improving ICT security.

2.11 The NSW RFS is committed to maintaining appropriate levels of security over all its systems.

3 Related documents

- *Privacy and Personal Information Protection Act 1998*
- NSW Government ICT Strategic Plan
- NSW Government ICT Assurance Framework
- NSW Government Information Management Framework
- NSW Government Investment Policy and Guidelines, Feb 2014
- NSW Government Procurement Policy Framework
- NSW Treasury Circular 10/13 Gateway Review System
- Department of Finance and Services DP0036 v3.0 Acceptable Use Policy
- Service Standard 1.1.2 Discipline
- 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
- Service Standard 5.1.10 Fire Control Centre Accommodation and Facilities
- Service Standard 5.1.11 Standard Brigade Stations
- Policy 3.1.1 Communications
- Policy P3.2.4 Working from Home
- 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 P7.1.1 Project, Program and Portfolio Management
- Policy P7.1.4 NSW RFS Planning and Reporting
- NSW RFS Corporate Plan 2014-2021
- NSW RFS Enterprise Architecture
- NSW RFS ICT Strategic Plan
- ICT Exemption and Exception Business Justification process
- ICT Exemption and Exception Business Justification template

4 Amendments

AMENDMENT DATE	VERSION NO	DESCRIPTION
14 December 2009	1.0	Initial release
2 June 2011	1.1	› Repealed and remade P5.1.1 v1.0 › Reviewed to include addition of clause 3.4
1 June 2016	2.0	› Repealed and remade P5.1.1 v1.1 › Repealed P5.1.3 ICT Security v1.0 and incorporates and updates content › Clauses 2.4 and 2.7 in P5.1.1 v1.1 removed › Clause 2.10 added in ICT Equipment Exceptions › Minor change to ICT Standards Exception Process diagram
30 June 2017	2.1	› Repeals and remakes P5.1.1 v2.0 › Amends clause 2.4

SOP P5.1.1-1
ICT EQUIPMENT STANDARDS AND SECURITY

1 Purpose

1.1 This Standard Operating Procedure (SOP) details the procedures the NSW RFS will implement to ensure standard ICT equipment and ICT security across the Service.

2 Procedures

ICT Planning

2.1 Staff are requested to engage ICT in the planning and procurement processes, as per P4.1.3 Procurement policy, for all current, new and/or modified ICT equipment, software, and services.

2.2 The procurement of new/modified equipment will be subject to ICT planning, research and testing.

2.3 ICT Management allocates resources in advance for the financial year ahead based on identified projects and requests. Although ad hoc requests may still arise, managers are asked to provide reasonable notice to the ICT Service Desk for any ad hoc requests, e.g. audits and exception reviews.

Online Quotes

2.4 All ICT procurement will be done using NSW Government online quoting system (eQuote) and suppliers must be part of NSW Government pre-qualification scheme(s).

2.5 Any exception to clause 2.4 must be approved, in writing, by the Chief Information Officer and the Chief Procurement Officer.

ICT Equipment Standards

2.6 ICT equipment which has exceeded its useful life and/or no longer complies with the ICT standards should be considered, in planning terms, as a replacement priority.

2.7 ICT equipment will be installed with the NSW RFS ICT Standard Operating Environments (SOE) and the current version of standard software.

2.8 ICT Assets are to be managed in the approved asset management system (currently SAP Enterprise Asset Management).

ICT Equipment Exceptions

2.9 The process for exceptions is initiated by logging a ticket with the ICT Service Desk once the relevant Manager's approval has been granted.

2.10 All approved exceptions will be reviewed periodically by ICT. If necessary any related ICT standards and processes will also be reviewed and updated.

2.11 ICT equipment found not to comply with standards or not covered by an approved equipment assessment may be removed from the NSW RFS' network.

RFS Risk Management Approach

2.12 ICT security controls and objectives will be set through a methodical assessment of risks in accordance with the NSW RFS' enterprise-wide risk management approach.

2.13 Expenditure on ICT security controls needs to be balanced against the business harm likely to result from security failures. The results of periodic risk assessment shall help to guide ICT and determine the appropriate management action and priorities for managing ICT security risks, and for implementing controls selected to protect against these risks.

Compliance Framework

2.14 ICT security controls shall be determined and applied in compliance with all relevant legislation, government directives, and NSW RFS policies and service standards. Other ICT policies provide specific ICT security guidance, which should be considered together with this policy.

Education and Awareness

2.15 All ICT users within the NSW RFS shall receive periodic education and awareness updates regarding their roles and obligations in helping to preserve appropriate security over ICT, and how to report identified security weaknesses and incidents.

Business Continuity

2.16 ICT shall document, maintain, test and continually improve ICT Disaster Recovery Plans for each identified ICT system so that they can be recovered and restored within acceptable timeframes.

2.17 Managers are responsible for their respective unit's Business Continuity Plans (BCP).

Reporting ICT Security Incidents

2.18 All users have an obligation to report all identified and suspected ICT security incidents to the ICT Service Desk immediately.

ICT Security Management Responsibilities

2.19 Whilst the ICT section retains responsibility to ensure that all ICT systems within its area of control are maintained at appropriate levels of security, it remains the responsibility of staff across the NSW RFS to comply with the following ICT security directives. (Volunteers and visitors are required to comply with security responsibilities outlined in the relevant service standards):

a. **Connection of ICT equipment to the NSW RFS Corporate network**

Non standard equipment should not be connected to the NSW RFS network unless a business justification is submitted and approved in accordance with the ICT exemption/exception process.

b. **Acceptable use of ICT systems and devices**

All staff must comply with the terms set down in Policy P5.1.2 Acceptable Use of ICT.

c. **Integrity of NSW RFS ICT**

Staff must not tamper with any back-up, virus protection or security software which has been applied to NSW RFS desktop computers, mobile computing and communications devices. Where these devices are the property of the NSW RFS, users are not permitted to make any changes to, or load any software onto, those devices unless a business justification is submitted and approved following the ICT exemption/exception process.

d. **Password management**

Staff are required to apply the following password management rules:

i. Keep passwords confidential at all times;

ii. Avoid keeping a paper record of passwords, unless this can be stored securely;

iii. Change passwords whenever a possible system or password compromise is suspected;

iv. Select quality passwords with a minimum length of six characters which are:

- Easy to remember but difficult to guess;
- Not based on anything somebody else could easily guess or obtain e.g. names, telephone numbers, and dates of birth, etc;
- Free of consecutive identical characters or all-numeric or all-alphabetical groups;

v. Change passwords when prompted by the system and avoid re-using or cycling old passwords;

vi. Do not share or disclose your password to anyone.

e. **Unattended computers**

Staff should either log-off or lock their computer if they leave their work area unattended.

f. **Software**

Loading non-approved software onto the NSW RFS network may only be undertaken after a business justification is submitted and approved in accordance with the ICT Exemption and Exception business justification process.

g. **Software Copyright**

Staff must not breach software copyright, licensing or intellectual property rights. The terms and conditions of all licensing agreements must be adhered to. All software and other applicable materials must be licensed and used in an appropriate manner.

Monitoring and logging

2.20 Use of ICT systems are monitored and logged by ICT. Refer to Policy P5.1.2 Acceptable Use of ICT for more information.

Review and assurance

2.21 The adequacy and effectiveness of ICT security will be reviewed on a periodic basis by ICT. The reviews will be assessed for accuracy through security audits undertaken by non ICT personnel.

Validation of access rights

2.22 Access rights will be periodically validated in accordance with Policy P5.1.2 Acceptable Use of ICT and ICT procedures.

Connection to external networks

2.23 NSW RFS equipment is not to be connected to any external network whilst it is simultaneously connected to the RFS network, until a business justification is submitted and approved in accordance with the ICT Exemption and Exception business justification process.

Connection from external networks

2.24 Connection of any external users or ICT systems to the NSW RFS network may only be established if an ICT Exemption and Exception business justification has been submitted and approved in accordance with the ICT exemption/exception process.

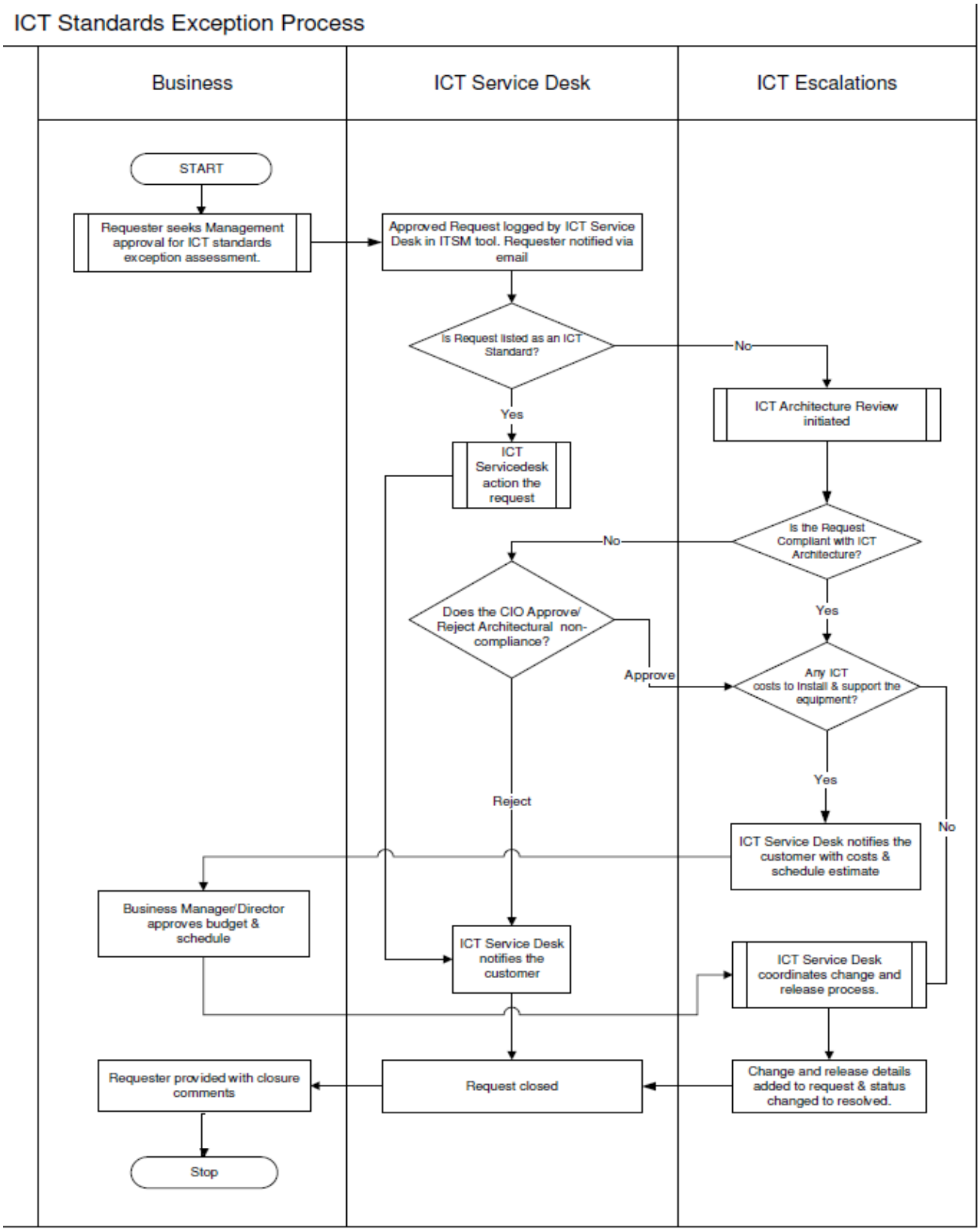
Malicious software protection

2.25 All NSW RFS ICT assets must be protected from malicious software, including computer virus infection. Refer to Policy P5.1.2 Acceptable Use of ICT for more information on how inappropriate use of ICT will be monitored and treated.

Non compliance with this policy

2.26 Violations of this policy, depending on severity and nature, will be actioned as outlined in Policy P5.1.2 Acceptable Use of ICT.

ICT Standards Exception Process



3 Related forms

- None