Policy P5.1.1
ICT Equipment Standards

Version	3.1
SOPs	SOP P5.1.1-1 ICT Equipment Standards
Policy Owner	Executive Director Technology, Finance & Legal
Policy Contact	Director ICT/Chief Information Officer
Approval Date	31 July 2024
Next Review	31 July 2029

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.

1.2. The 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 these assets from a wide range of threats. Security of RFS ICT assets is managed in accordance with policy P5.1.3 Information Security Management.

1.4. This policy:

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

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

2. Policy

Equipment

2.1. The selection and procurement of new and replacement ICT equipment is to be in accordance with the RFS Procurement Framework, including P4.1.3 Procurement and its accompanying Procurement Manual, and ICT Standards, including but not limited to the RFS Enterprise Architecture, Government policy and 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.

2.3. The procurement of all ICT equipment intended for use on the RFS network is to be in accordance with policy P4.1.3 Procurement and its accompanying Procurement Manual. This

includes but is not limited to ensuring maintenance, support and confidentiality agreements and standard replacement cycles are in place, including any arrangements with third party providers.

2.4. Procurement stages including planning, negotiation, demonstration, proof of value, proof of concept stages are subject to confidentiality and non-disclosure arrangements, including the secure disposal of test and sample data. The RFS may request assurance of this disposal.

2.5. All computers used on the RFS network must use RFS ICT developed standard operating environment (SOE) and associated licensed software. For exceptions, refer to SOP P5.1.1 – 1 ICT Equipment Standards. 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 RFS network by following the ICT Standards Exception process detailed at SOP 5.1.1-1 of this policy.

2.7. All ICT equipment is to be replaced at the expiry of the warranty period, i.e. four years for desktops and laptops, and three to five years for other ICT equipment.

Data

2.8. Prior to disposal of ICT equipment, all data stored on RFS equipment and devices is to be disposed of in accordance with ICT Standards. Further information on the disposal of RFS data can be obtained from the ICT Serve Desk.

3. Document control

Release history

Version	Date	Summary of changes
1.0	14 December 2009	Initial release
1.1	2 June 2011	Repealed and remade P5.1.1 v1.0 Reviewed to include addition of clause 3.4
2.0	1 June 2016	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 removed Clause 2.10 added in ICT Equipment Exceptions Minor change to ICT Standards Exception Process diagram
2.1	30 June 2017	Repeals and remade P5.1.1 v2.0 Amends Clause 2.4
3.0	17 May 2019	Repealed and remade P5.1.1 v2.1 Change of title from “ICT Equipment Standards and Security” to “ICT Equipment Standards” Content relating to ICT Security removed into reinstated P5.1.3 Information Security Management v2.0 – i.e. title, clauses 2.8-2.11, SOP P5.1.1-1 clauses 2.12-2.19, 2.21 of P5.1.1 v2.1
3.1	31 July 2024	Minor review to update branding, role titles and minor amendments to reflect current practice.

Approved by

Name	Position	Date
Rob Rogers AFSM	Commissioner	31 July 2024

Related documents

Document name
NSW Cyber Security Policy
Service Standard 1.1.14 Personal Information and Privacy
Service Standard 5.1.3 Communication Systems
Policy P4.1.3 Procurement
Policy P4.1.9 Communications – Mobile and Data Devices
Policy P5.1.2 Acceptable Use of Information and Communication Technology (ICT)
RFS Internal ICT document library
ICT Exemption and Exception Business Justification process

SOP P5.1.1-1
ICT Equipment Standards

1. Purpose

1.1. This Standard Operating Procedure (SOP) provides detail on the procedures to ensure standardised ICT equipment across the Service.

2. Procedures

ICT Planning

2.1. Staff are requested to engage ICT in the planning and procurement process, as per Policy P4.1.3 Procurement, 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, including a cyber risk assessment.

2.3. ICT Management allocates its 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), in accordance with the RFS Procurement Framework.

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

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 when developing cost centre budgets.

2.7. ICT equipment will be installed with the 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 RFS network.

Monitoring and logging

2.12. Use of ICT equipment and systems is monitored by ICT. Refer to Policy P5.1.2 Acceptable Use of ICT for more information.

Validation of access rights

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

Connection to external networks

2.14. 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

2.15. Connection of any external users or ICT systems to the 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

2.16. All RFS ICT assets must be protected from malicious software, viruses and other cyber threats. 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

2.17. Breach of this policy, depending on severity and nature, may be subject to the provisions of the Government Sector Employment Act 2013

2.18. Breaches of contracted and other arrangements may result in legal or other action.

3. Related documents

3.1. None