NSW RURAL FIRE SERVICE

SERVICE STANDARD 1.4.4
VOLUNTEER MEMBER AND VISITOR ACCESS TO NETWORK SERVICES AND DATA

ITEM	DESCRIPTION
Version Number	1.0
SOPs	› SOP 1.4.4-1 Volunteer Member and Visitor Access to Network Services
Owner	Executive Director, Infrastructure Services
Contact	Director, ICT
Approved Date	20 August 2019
Effective Date	20 August 2019
Next Review	20 August 2024
Document Control	Electronic - Printed Copies are Uncontrolled

1 Purpose

1.1 Information and Communications Technology (ICT) solutions, equipment and data are valuable corporate assets which must be safeguarded at all times from malicious attack, unauthorised access and inappropriate use. Failure to do so may result in the degradation of NSW RFS information assets, affect the ability of the NSW RFS to carry out its core functions, lead to loss of reputation, or legal actions.

1.2 It is recognised that during incidents when they may be part of an Incident Management Team (IMT), and at various other times, volunteer members and visitors require network access to undertake tasks related to their allocated IMT role.

1.3 This Service Standard provides the framework for authorised volunteer members and visitors to access and use NSW RFS network services and data located on the NSW RFS wide area network and local area networks

1.4 This Service Standard is applicable to volunteer members and visitors only. NSW RFS staff should refer to P5.1.2 Acceptable Use of ICT.

2 Definitions

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

a. **Citrix:** Remote network access software.

b. **ICT:** Information and Communications Technology.

c. **IMT:** Incident Management Team.

d. **ISO/IEC**: a joint technical committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its purpose is to develop, maintain and promote standards in the fields of information technology (IT) and Information and Communications Technology (ICT).

e. **Manager:** Person in charge of a District, Section or Department.

f. **MyRFS:** A website that allows volunteer members internet access to the NSW RFS.

g. **PC:** Personal Computer (Including laptops, desktops and mobile devices).

h. **RMS:** NSW RFS Resource Management System.

i. **SSL:** is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

3 Policy

3.1 Volunteer member and visitors given access to the NSW RFS' network services and data are required to abide by all relevant NSW RFS Policies and Service Standards, Government guidelines and legislation. They are also required to abide by the principles of non-disclosure of information and appropriate use of NSW RFS resources. The NSW RFS network services and data are provided for business purposes.

3.2 All use of the NSW RFS network services and data must be lawful, efficient and ethical. Any identified use of network services or data thought to be inconsistent with NSW RFS service standards or in violation of any Australian or State regulations or laws may be referred to an external agency and/or regulator for investigation, and may result in disciplinary (volunteer) or misconduct (staff) action., Authorised volunteer members and visitors are granted access to ICT to undertake their roles and responsibilities. Access is determined by the relevant manager and/or Manager of ICT.

3.3 Access to authorised volunteer members and visitors is granted to pre-existing network infrastructure only. The access does not infer that network infrastructure will be extended or new equipment purchased for such access.

3.4 Monitoring, logging and SSL visibility tools are used by the NSW RFS on all ICT systems and services. The user accepts this condition as part of their login conditions to the NSW RFS systems and services.

3.5 In accordance with the NSW Government Cyber Security Policy (CSP) and the international standard for Information Security Management Systems (ISO/IEC 27001/2013), the NSW RFS is implementing a number of information security controls to reduce the risk of unauthorised access to sensitive NSW RFS information. One of the measures is to reduce the number of generic network access usernames and passwords including those used by volunteer members and visitors, is being reduced.

3.6 As part of this reduction, and where the capability exists and has been agreed with District Managers, District Staff can provide volunteer members with network access through ICT systems, using the volunteer's MyRFS user name and password.

NOTE: Districts or Sites wanting to clarify if they have the ability to give their volunteer members this access can do so by contacting the SAP Team SAP@rfs.nsw.gov.au.

3.7 Visitors and volunteer members forming part of an IMT and not covered by the network access capability will be provided with a site-specific generic username and password with a pre-determined expiration date.

3.8 Once an incident has been terminated and the IMT formed for that specific incident has completed its tasks and been disbanded, the District Manager and/or Incident Controller is responsible for notifying the ICT Service Desk that the site specific generic account can be disabled. Passwords are reset once a request is received to re-enable a generic account.

3.9 Visitors from other agencies who work in the State Operations Centre or Major Incident Logistics at NSW RFS Headquarters will be provided with a generic network account based on their agency's name.

Individually named accounts

3.10 For volunteer members that may require "staff level access" (with the exception of SAP) for day-to-day business within a District, an individually named account may be used. These will be the exception rather than the rule. Approval is required from a Regional Manager before individually named volunteer member accounts are created and they will need to demonstrate that the required level of access cannot be

provided through other network access solutions. Volunteer members requiring staff level access will be provided with:

a. NSW RFS email addresses with a 2GB limit, that will be identified as firstname.surname@rfs.nsw.gov.au;

b. The NSW RFS Intranet; and

c. Relevant corporate drives, for example, Headquarters “G Drive”.

3.11 Individually named volunteer member accounts and site-specific generic accounts (except for those of fire investigators) are set automatically to be disabled after twelve months. They can be re-enabled by the ICT Service Desk on receipt of a written request from the District Manager or the Senior Fire Investigator / Fire Investigations Manager.

3.12 Specialist IMT volunteer member roles such as Fire Behaviour Analysts, Fire Investigators, Aviation Specialists, Safety, Media and Public Liaison Officers, will be set up with an individually named account. The District Manager is authorised to approve this request. Volunteer members undertaking such specialist roles will be granted access to:

a. NSW RFS email addresses with a 4GB limit, that will be identified as firstname.surname@rfs.nsw.gov.au;

b. The NSW RFS Intranet;

c. Relevant corporate drives, for example, Headquarters “G Drive”; and

d. Remote access to NSW RFS systems through Citrix.

3.13 General IMT volunteer member roles such as: Logistics Officer, Management Support and the like where the role has been added to the volunteer record (by the District Manager), will be able to log on with their MyRFS account. Access will be granted to:

a. RFS PCs and access applications via desktop shortcuts (given they already have access to the online applications);
b. Local Printers;
c. L:\Volunteers, L:\\Gis; and
d. Incident Management Procedures on the intranet (cut down version of staff intranet) and Internet.

3.14 All Volunteer members and visitors not mentioned in the above clauses will not be provided access to the following:

a. NSW RFS email addresses;

b. The NSW RFS Intranet;

c. Corporate drives, for example, Headquarters “G Drive”; and

d. Remote access to NSW RFS systems through Citrix.

3.15 Passwords are the responsibility of the password owner and must not be divulged. Due to the potential security risk to the organisation, if it is found that passwords have been divulged, disciplinary action may result.

3.16 Users of non NSW RFS laptops, tablets, phones or other devices with a wireless capability may connect to an NSW RFS provided wireless network using a user name and password provided on request by the ICT Service Desk or via Guest Wireless Self Service provisioning. This access enables visitors and volunteers to browse the internet and must be in accordance with Clauses 3.1 and 3.2.

Volunteer Member and Visitor rights and responsibilities

3.17 The NSW RFS prohibits the use of network services to:

a. intentionally create, send or access information that could damage the NSW RFS’ reputation, be misleading or deceptive, result in victimisation or harassment, lead to criminal penalty, or be reasonably found to be offensive, obscene, threatening, abusive of defamatory;

b. operate a business, usurp NSW RFS business opportunities or generate personal income (including through gambling);

c. send, receive, print or otherwise disseminate, without appropriate authorisation, proprietary data or other confidential information of the NSW RFS;

d. gain unauthorised access to, or make unauthorised changes to, programs or data, cause disruption to, or unacceptable levels of outages to, critical NSW RFS business systems or otherwise compromise the integrity of sensitive NSW RFS data;

e. install non-approved software onto NSW RFS networked PCs without the express written permission of ICT;

f. make copies of any software licensed to the NSW RFS, or load any software licensed to the NSW RFS onto personal computers, laptops, servers or any other device not owned by the NSW RFS;

g. breach copyright law or any law or regulation relating to intellectual property;

h. violate the privacy of other individuals;

i. use for games, streaming multimedia or other non-business, high-bandwidth activities not related to agreed roles and/or responsibilities, or without prior approval; or

j. use in any other inappropriate manner including, but not limited to, any use of NSW RFS equipment or services for intentionally transmitting, communicating or accessing pornographic or sexually explicit images, text or other offensive material, or any other material which may discriminate against, harass or vilify any other person.

Manager responsibilities

3.18 Managers who wish to authorise access to volunteers and visitors are responsible for:

a. ensuring that all relevant signed ICT access forms are forwarded to the ICT Service Desk;

b. monitoring acceptable use and if necessary, request from ICT an internet usage report;

c. ensuring authorised volunteers and visitors have the required access to perform their role;

d. terminating access rights for volunteers and visitors where their task is finished earlier than planned; and

e. the management of generic district accounts and the associated user name and password is the responsibility of the District Manager. ICT can re-set this account and password if required.

4 Related documents

- *Privacy and Personal Information Protection Act 1998*
- *Copyright Act 1968*
- NSW Government ICT Assurance Framework
- NSW Government Information Management Framework
- 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
- Security Standard ISO/IEC 27001 Information Security Management System
- Department of Finance and Services DP0036 v3.0 Acceptable Use Policy
- Policy P5.1.1 ICT Equipment Standards
- Policy P5.1.2 Acceptable Use of ICT
- Policy P5.1.3 Information Security Management
- Service Standard 1.1.2 Discipline
- Service Standard 1.1.7 Code of Ethics
- Service Standard 1.1.14 Personal Information and Privacy
- Service Standard 1.1.42 Respectful and Inclusive Workplace

- NSW RFS Password Standards
- NSW RFS Data Security Standards

5 Amendments

AMENDMENT DATE	VERSION NO	DESCRIPTION
4 March 2005	1.0	• Initial release as SS 1.1.26 Volunteer and Visitor Access to Network Services and Data
31 March 2009	1.1	• Repealed and updated SS 1.1.26 v1.0 • Update ICT Provisions
20 August 2019	1.0	• Repeals and remakes SS 1.1.26 v1.1 • Change of title to Volunteer Member and Visitor Access to Network Services and Data • Renumbered to SS 1.4.4 v1.0 to align with the Service Standard Index categories • Updated to align with current organisational structure and processes, and changes to ISO standard and technology

SOP 1.4.4-1

VOLUNTEER MEMBER AND VISITOR ACCESS TO NETWORK SERVICES

1 Purpose

This Standard Operating Procedure (SOP) details the procedures for the NSW RFS to ensure acceptable volunteer member and visitor access to network services and data.

2 Procedures

2.1 District sites with the capability can provide a volunteer member with IMT qualifications and experience with network access through ICT systems as long as they have a MyRFS username. The process is recommended as part of the pre-season checking process.

2.2 It is the responsibility of the District Manager to ensure the appropriately trained and qualified volunteer members are added. Sites wanting to clarify if they have the ability to give their volunteer members access through ICT systems can do so by contacting the SAP Team SAP@rfs.nsw.gov.au .

2.3 The volunteer member access capability provides access to the following:

a. Incident Management Procedures;

b. Internet;

c. Local Printers;

d. Local L: drive (file shares on local district server);

e. Shortcuts to NSW RFS applications; and

f. Microsoft Office.

2.4 Access into SAP applications is not available for volunteer members at this time. If a District is seeking permission for a volunteer member in their District to have SAP access, they should contact the Manager ICT Products for advice.

2.5 Access provided to volunteer members as an IMT Officer (via SAP Portal) will be removed by ICT once a year, one month after the end of the fire season, as a security measure. It then becomes the responsibility of the District Staff to re-add their access for Volunteer members requiring network access during the pre-season planning process or as required. All other individually named volunteer member accounts and site-specific generic accounts created will comply with a validity period of twelve (12) months as stated in 3.11 of the Service Standard.

2.6 Sites without the capability, requiring network access for volunteer member and visitors will need to request a site-specific generic username and password through their District Manager or Incident Controller.

2.7 All Managers should log in a local register the use of generic usernames for the purposes of an audit (if requested) as well as for evidence in the event of an information security incident or breach. The building visitor log is an acceptable log for generic agency account usage in the State Operations Centre;

2.8 The District Manager should ensure that the volunteer/visitor read and sign a copy of the relevant ICT access form, and agree to acceptable use of internet prior to enabling access. A copy of any completed forms should be kept at a district level and also sent to ICT with the request for generic access.