Service Standard 1.1.26
Volunteer and Visitor Access to Network Services and Data

Date of Issue	31 March 2009
Version Number	1.1

1. Purpose

This Service Standard is the framework for access and use of RFS network services and data located on the RFS wide area network and local area networks by authorised volunteers and visitors.

2. Policy

2.1 Information Communications and 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 RFS information assets, affect the ability of the RFS to carry out its core functions, lead to loss of reputation, or legal actions.

2.2 It is recognised that during incidents when they may be part of an Incident Management Team ("IMT"), and at various other times, volunteers and visitors require network access to complete tasks related to their role.

2.3 In accordance with security standard ISO 27001/2, the RFS is reducing the number of generic network access usernames and passwords including those used by volunteers and visitors.
As part of this reduction, and where the capability exists and agreed with district managers, district staff can provide volunteers with network access through ICT systems, using the volunteer's MyRFS user name and password.

NOTE: **Sites wanting to clarify if they have the ability to give their volunteers this access can do so by contacting the ICT Service Desk Co-ordinator**.

2.4 Visitors and volunteers forming part of an IMT and not covered by the network access capability will be provided with a site-specific generic username and password. Acceptable use of generic usernames and passwords are the responsibility of the district manager.

2.5 Once an incident has been terminated and the IMT has completed its tasks and disbanded, the district manager is responsible for notifying ICT that the site specific generic account can be disabled. Passwords are reset once a request is received to re-enable a generic account.

2.6 Visitors from other agencies who work in the State Operations Centre or Interstate Liaison Unit at Headquarters will be provided with a generic network account based on their agencies' names. These accounts are owned and managed by the Manager State Operations.

2.7 For volunteers that may require staff level access, 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 and visitor network accounts are created. Regional Managers will need to demonstrate to ICT that the required level of access cannot be provided through other network access solutions.

2.8 Individually named volunteer accounts (except for those of fire investigators) are set automatically to be disabled after three months. They can be re-enabled by ICT on receipt of a request from the district manager.

2.9 Volunteers (except for fire investigators) and visitors network access will not provide access to the following, (see 2.11 for exceptions):

(a) RFS emails addresses;

(b) The full RFS Intranet;

(c) Corporate drives, for example, drive G; and

(d) Remote access through Citrix.

2.10 In the case of volunteer fire investigators, individually named accounts will be set up as they require a standard suite of agreed products. This will require approval from the Regional Operations Officer (Fire Investigation) or Operations Officer, Fire Investigation by way in accordance with the current ICT access control procedures.

2.11 On completion of the ICT access control procedures , the volunteer fire investigators will be provided with:

(a) an RFS email account;

(b) corporate drive access; and

(c) Citrix.

2.12 Passwords are the responsibility of the password owner and should 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.

2.13 Volunteers and visitors given access to the RFS' network services and data are required to abide by all relevant 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 RFS resources. The RFS' network services and data are provided for business purposes. All use of the RFS' network services and data must be lawful, efficient and ethical. Any identified use of network services or data thought to be inconsistent with RFS service standards or in violation of any Australian or State regulations or laws could result in disciplinary action, and a range of penalties, including dismissal or legal prosecution.

2.14 Non RFS laptop users with a wireless capability can connect to an RFS provided wireless network using a user name and password provided on request by the ICT Service Desk. This access enables visitors and volunteers to browse the web (see clause 2.13).

2.15 ICT resources are limited in capacity. Authorised volunteers and visitors are granted access to ICT to complete their roles and responsibilities. Access is determined by the relevant business owner and/or ICT manager.

2.16 Access to authorised volunteers 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.

Volunteer and Visitor rights and responsibilities

2.17 The RFS prohibits the use of network services to:

- **(a)** intentionally create, send or access information that could damage the 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 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 RFS;
- **(d)** gain unauthorised access to, or make unauthorised changes to, programs or data, or otherwise destroy the integrity of RFS data;
- **(e)** import or use executable programs within the RFS' network, or download programs from the Internet without the express written permission of Information Services;

(f) make copies of any software licensed to the RFS, or load any software licensed to the RFS onto personal computers, laptops, servers or any other device not owned by the 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 RFS equipment or services for intentionally transmitting, communicating or accessing pornographic or sexually explicit material, images, text or other offensive material, or any material which may discriminate against, harass or vilify any other person.

Manager responsibilities

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

(a) selecting appropriately skilled volunteers and visitors who are able to abide by the requirements of the RFS;

(b) ensuring that all relevant signed ICT access forms are copied and stored by districts before they are forwarded to ICT;

(c) monitoring acceptable use;

(d) logging generic user account usage;

(e) ensuring authorised volunteers and visitors have the required access to perform their role;

(f) terminating access rights for volunteers and visitors where their task is finished earlier than planned; and

(g) Changing generic account passwords at the start of an IMT and disabling accounts at completion of their assignment.

3. Links

- SOP 1.1.26-1 Volunteer and Visitor Access to Network Services
- Security Standard ISO 27001/2 (http://www.iso.org)
- Policy P 3.1.2 Harassment
- Service Standard 1.1.2 Discipline
- Service Standard 1.1.14 Personal Information and Privacy
- Service Standard 1.1.7 Code of Ethics
- Office of the NSW Privacy Commissioner *Privacy and Personal Information Protection Act 1998*

4. Who is responsible for implementing the Service Standard?

Director Infrastructure Services

5. Amendments

Updated ICT provisions	31 March 2009

SOP SS1.1.26-1
Volunteer and Visitor Access to Network Services

This SOP forms part of	SOP SS1.1.26 Volunteer and Visitor Access to Network Services

1. Purpose

This Standard Operating Procedure ("SOP") details the procedures the RFS will use to ensure acceptable volunteer and visitor access to network services and data.

2. Procedures

2.1 District sites with the capability can provide a volunteer with IMT qualifications and experience with network access through ICT systems as long as they have a MyRFS username. The process takes approximately one hour to complete and is recommended as part of the pre-season checking process. It is the responsibility of the district manager to ensure the appropriately trained and qualified volunteers are added. Sites wanting to clarify if they have the ability to give their volunteers access through ICT systems can do so by contacting the ICT Service Desk Co-ordinator.

2.2 The Volunteer 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 RFS applications; and

(f) MS Office.

2.3 Access provided to volunteers as per clauses 2.1 and 2.2 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 Volunteers requiring network access during the pre season planning process or as required.

2.4 Sites without the capability, requiring network access for volunteer and visitors will need to request a site specific generic username and password through their district manager or incident controller.

2.5 All Managers should log in a local register the use of generic usernames for the purposes of an audit (if requested). The building visitor log is an acceptable log for generic agency account usage in the State Operations Centre;

2.6 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.

Acronyms and Definitions

IMT – Incident Management Team

ICT – Information Communication and Technology

RMS – RFS Resource Management System

MyRFS – Volunteer Extranet.

Manager – Person in charge of a district, section or department