Roosevelt Fire District

Section:	**Policy:**
Operations	Information Technology

1. Acceptable Use

1.0 Overview

Roosevelt Fire District is committed to protecting our employees, Commissioner's, volunteer's and the Fire District from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Roosevelt Fire District. These systems are to be used for business purposes in serving the interests of the Fire District, in the course of normal operations.

Effective security is a team effort involving the participation and support of every District employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Roosevelt Fire District. These rules are in place to protect the employee and the District. Inappropriate use exposes the Fire District to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, volunteers, Commissioners, and other workers at Roosevelt Fire District, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Roosevelt Fire District.

4.0 Policy

4.1 General Use and Ownership

1. While Roosevelt Fire District's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the District systems remains the property of Roosevelt Fire District.

2. For security and network maintenance purposes, the Secretary and Treasurer may monitor equipment, systems and network traffic at any time.

3. Roosevelt Fire District reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
2. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 20 minutes or less, or by logging-off when the host will be unattended.
3. Because information contained on portable computers is especially vulnerable, special care should be exercised.
4. Postings by employees from a Roosevelt Fire District email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Roosevelt Fire District, unless posting is in the course of business duties.
5. All hosts used by the employee that are connected to the Roosevelt Fire District Internet/Intranet/Extranet, whether owned by the employee or Roosevelt Fire District, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Roosevelt Fire District authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Roosevelt Fire District-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Roosevelt Fire District.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Roosevelt Fire District or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others.
6. Using a Roosevelt Fire District computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Roosevelt Fire District account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of

which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, Roosevelt Fire District employees to parties outside Roosevelt Fire District.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Roosevelt Fire District's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Roosevelt Fire District or connected via Roosevelt Fire District's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Computer Disaster Recovery Plan

6.2 Data Backup and Restoration Plan: Data is backed up daily onsite with 4 hard drives that mirror each other. Every night there is a backup created and stored off site by Enveloc, the company the District contracts with for this service.

6.1 Plans must be updated

Review all plans annually so changes in the Districts situation can be incorporated.

Board approved: 02/15/15 Last Revision 01/15