

U.S. FISH AND WILDLIFE SERVICE -- REGION 6**RULES OF BEHAVIOR (ROB) FOR NETWORK RESOURCES****INTRODUCTION**

Electronic mail and the Internet, along with the computers that enable them, have become essential to global business practices and intrinsic to our culture. Many people have computers and an Internet connection at home as well as on the job. It has become a virtual jungle out there, with computer security breaches worldwide all too common. It is estimated that 1 out of 10 laptops will be stolen or lost each year (Gartner Group), with 47% of those stolen from the workplace, and 97% of stolen computers will never be recovered (FBI).

It is necessary to have a resource management strategy in place to guide employees through appropriate use, and to help Service network resources remain secure from both inadvertent and intentional harm. This document lays out responsibilities and rules of behavior for use of Service network and computer resources.

These Rules of Behavior (ROB) are mandated by OMB A-130, Appendix III, and specify responsibilities and expected behavior that all individuals (employees and contract staff) must follow if they have access to or use the DOI Enterprise Services Network (ESN), Service Wide Area Network (SWAN), or the Internet using any Service-owned computer equipment. These ROB also outline standard practices needed to ensure safe, secure, and reliable use of information and information systems.

Failure to follow these ROB can result in disciplinary action. At the discretion of R6 management, penalties for non-compliance may include, but are not limited to, a verbal or written warning, removal of system access, reassignment to other duties, demotion, suspension, termination, and possible criminal and/or civil prosecution.

These ROB do not replace existing security policies or directives. Rather, they supplement and further articulate existing security policies and practices, and are consistent with the following directives:

- DOI Departmental Manual 375, Chapter 19;
- DOI Information Security Plan;
- DOI Security Handbook; and
- Region 6 System Security Plan.

RESPONSIBILITIES

The Federal Government policy has been relaxed in many areas of network and computer usage in an effort to promote a more knowledgeable workforce. It has become acceptable practice for employees to use their computer and network resources in educational pursuit on their personal time, as long as it is not incurring additional costs to the Service. This relaxation makes it more crucial for each employee to know the rules for appropriate use. Each category of employee listed below has increasing responsibilities, and must follow the rules of appropriate use detailed in this document.

A. ALL EMPLOYEES:

1. Must attend an IT Security Awareness Training session once a year and sign a Statement of Responsibility form.
2. Must abide by the rules of appropriate use of Region 6 network resources, as stated in this document.

3. Are responsible for management of any vital records in their care.
4. Are responsible for backup of information residing on their computer.
5. Must guard network security and aid in computer software virus/malware avoidance.
6. Must represent the Service in a responsible manner in any Internet transaction.

B. SUPERVISORS AND MANAGERS:

1. Are responsible for knowing and enforcing the rules for appropriate use and protecting the Service's assets from waste, fraud and abuse.
2. Are responsible to ensure that their employees receive proper IT Security Awareness Training and have signed a Statement of Responsibility form.
3. Are responsible for making the final determination as to the appropriateness of their employees' use of the Internet in the event of abuse of this policy or in order to meet management needs and mission objectives. This shall include the acceptability of Internet sites visited and the determination of personal time versus official work hours.
4. Are responsible to notify the IRTM Office in the event of inappropriate employee behavior. IRTM will notify the ARD-BA, who will involve the appropriate offices/entities to determine if disciplinary or other action should be taken.

C. NETWORK AND COMPUTER PROFESSIONALS:

1. Conduct IT Security Awareness Training sessions, updating information and issuing security event warnings through electronic mail or other appropriate method.
2. Provide notification that all network and computer activities are subject to monitoring.
3. Keep the electronic mail moving, which may entail removal of mail messages that contain viruses, non-work-related material, or exceed the established size restriction controls.
4. Keep network resources secure, which may entail removal of files that represent a threat to the security of network resources, setting required security features, and implementing encryption.
5. Keep network performance acceptable, which means that network activity is subject to monitoring and some activities subject to being curtailed.
6. Are responsible to notify IRTM and ARD-BA of any improper use detected through network and electronic mail monitoring or other means. ARD-BA will discuss such employee usage with the proper supervisor, including potential disciplinary action and repercussions of continued abuse.
7. Provide technical support in investigation of security incidents.
8. Take the lead in security incidents involving outside attacks to the network.

APPROPRIATE USE AND BEHAVIOR

PRIVACY

Electronic mail within the Service is not private and should not be used to communicate sensitive information unless the information is encrypted using an approved encryption algorithm. All messages are subject to review by an employee's supervisors or by network administrators, electronic mail managers or other support staff as necessary to maintain effective communications. All Service systems and network functions, including Internet access, are subject to monitoring by supervisors and/or individuals charged with the maintenance, management, and security of these systems.

USER IDS AND PASSWORDS

User IDs and passwords are required of all employees for access to the Service network (ESN, the Enterprise Services Network), the Internet, and other Service systems. Each employee must be uniquely identifiable by his/her unique ID/password. Employees and managers are jointly responsible

for ensuring that timely notice is given to the IRTM Office when any employee leaves the Service, transfers, or for some other reason should be removed from network or system access.

Each employee is accountable for all actions associated with the use of their User ID and password, and will be held accountable for unauthorized actions found to be intentional, malicious, or grossly negligent. The employee is therefore charged to know the rules for creating and managing good passwords, for protecting these passwords from compromise, and for alerting his/her supervisor immediately if a compromise is suspected.

All Service employees are prohibited from accessing or attempting to access systems or information for which they are not authorized, or changing access controls to allow themselves or others to perform actions outside their authorized privileges. To minimize the risk of unauthorized access, employees must **activate some form of password-protected screen saver** if they will be away from their workstations for more than a few minutes.

Passwords to all Service systems are considered private. Employees will not share their passwords unless specifically directed to do so by their supervisor or other appropriate manager. Any manager who requires that an employee share a private password assumes responsibility for all activity that occurs under that password until such time as it is changed. This does not preclude a reasonable policy for password management to ensure continuity of operations. Such policies must be in writing and provide well-defined rules for use.

GENERAL INTERNET PRINCIPLES

The Service promotes Internet use that enables employees to perform Service missions and encourages its employees to develop Internet skills and knowledge. If an employee's supervisor determines that Internet access is in the best interest of the Government, the employee will be permitted, within the limits set forth below, to use the Internet to build his/her network search and retrieval skills. It is expected that employees will use the Internet to improve their job knowledge; access scientific, technical, and other information on topics which have relevance to the Service; and communicate with their peers in other Government agencies, academia, and industry. Employees should be aware that when access is accomplished using Internet addresses and domain names registered to the Service, they may be perceived by others to represent the Service. Employees are advised not to use the Internet for any purpose which would reflect negatively on the Service or its employees.

Federal computer systems are for Government use and not for personal use. All computers (servers, desktop computers, laptops/notebooks, and peripheral equipment), software license rights, the internal computer networks, and the information residing on them are business assets of FWS. Computer systems will display a logon banner similar to the following to advise users of FWS intentions to monitor the use of these systems:

“Warning...You are accessing U.S. Government information systems of the U.S. Department of the Interior, Fish and Wildlife Service. Access to these systems without approval by the appropriate authority or the use of these systems in excess of approved limits are in violation of Federal law and can subject the abuser to criminal and civil penalties. Users of these systems are subject to having all of their activities monitored and recorded. If such monitoring reveals possible evidence of criminal activity, the evidence obtained from such monitoring may be provided to law enforcement officials. Clicking OK or pressing a key to continue with the boot process is your acknowledgement you are aware of these terms.”

However, when certain criteria are met, Service employees are permitted to engage in the following activities:

1. During working hours, access job-related information, as needed, to meet the requirements of their jobs.
2. During working hours, participate in news groups and e-mail discussion groups (list servers), provided these sessions have a direct relationship to the user's job with the Service. If personal opinions are expressed, a disclaimer will be included stating that this is not an official position of the Service.
3. During personal time, retrieve non-job-related text and graphics information to develop or enhance Internet-related skills if the office pays a fixed rate for Internet access; that is, the access charge is usage insensitive. It is expected that these skills will be used to improve the accomplishment of job-related work assignments.
4. Employees are now permitted to send personal e-mail from their Service e-mail system, as long as no more than five people are addressed in each message.
5. Employees are now permitted to make personal purchases from the Internet on their personal time, as long as those purchases are not for personal commercial gain or do not involve push technology, such as that employed by stock market sites.

The following activities are prohibited for all Service network resources unless a specific exception is made by the Director:

1. Any form of partisan politics. This prohibition does not apply to Presidential appointees who have received Senate confirmation.
2. Personal commercial activities or any venture related to commercial gain or profit. This includes offering service or merchandise for sale or ordering non-work-related services or merchandise from on-line vendors, when related to personal commercial ventures.
3. Religious activities including newsletters, fund raising, proselytizing, prayer exchange, or activities related to the management of a religious institution.
4. Any illegal activity, Federal or State, as well as any activity prohibited by other Federal policy or that would bring discredit to the Service.
5. Accessing, retrieving, or printing text or graphic information which exceeds the bounds of generally accepted standards of good taste and ethics.
6. Engaging in any activity which would compromise the security of any Government information system.

WIRELESS NETWORKING

Mobile Broadband (802.11x) Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. However, there are risks associated with a wireless connection. Some of the risks are similar to those of wired networks, some are exacerbated by wireless connectivity, and some are new risks. Perhaps the most significant source of risks in wireless networks is the technology's underlying communications medium, the airwave. With the data traveling over the public airwaves, measures must be taken to ensure the confidentiality of the data. Because these measures are not always available, users must be informed of the risk. The use of wireless technology can further enhance convenience for users by providing wireless access points in locations such as hotels, airports, and public hotspots. Extra security precautions must be taken when mobile PCs are taken outside of the FWS office environment. Remote access to the FWS network by mobile computers can only be granted through the use of the ESN VPN

(Enterprise Services Network Virtual Private Network) connections, either through a local Internet Service Provider (ISP) or via a public wireless access point.

All usage of wireless networking capabilities must comply with the FWS "Wireless Broadband 802.11x Access Security Technical Implementation Guide" (STIG). Wireless networking capability is prohibited at all FWS facilities, and the **wireless connection must be disabled** when a computer is connected to a Service LAN.

ELECTRONIC MAIL

Service electronic mail is not private for many reasons. It is part of the Service's records and subject to Freedom of Information Act (FOIA) requests. If messages are sent over the Internet, they are (by default) sent in clear text and can be captured, or can end up at mail relay sites or in the wrong mailbox. Access by unknown parties can also be gained by replying to or forwarding mail. Care must be taken with sensitive information.

Many excellent resources are available via Internet mailing list communities. Employees must be judicious with their use. Employees may subscribe to an Internet mailing list that pertains to that employee's job with the permission of their supervisor. Posting messages or replying to messages from these lists or newsgroups from an "fws.gov" address could imply official content. The employee shall have clearance from their supervisor and the Office of External Affairs to express an official opinion, relying on Service policy pertaining to written documents. The employee will use a disclaimer when expressing a private opinion. Many of these problems can be avoided if an employee subscribes to Internet mailing lists as a private citizen through a non-Service electronic mail address.

THE WEB

Many interesting resources are available through websites. Some of them require a large amount of network bandwidth to use. Streaming audio (radio and music) and video (movie clips) are prohibited except in the pursuit of official business. While employees may play CDs on their computers, since this takes no bandwidth, they may not use the computer as a radio or television device. Use of stock market and weather software that pushes information to the computer is also prohibited.

Any questions on these Rules of Behavior, specific situations or uses, access to certain sites, etc., should be referred to the Regional IT Security Manager, Margaret Wolf in IRTM, 303-236-8116.

I have read and understand these Rules of Behavior governing my use of the Region 6 FWS R6ROLAN and agree to abide by them. I understand that failure to do so may result in disciplinary action being brought against me.

User Name (Please Print) _____

User Signature _____

Organization _____

Date _____