

**U.S. FISH AND WILDLIFE SERVICE -- REGION 6****WIRELESS USE POLICY****INTRODUCTION AND SCOPE**

This policy applies to all personnel, including those volunteers and government-funded contractors with security clearance, with access to or use of government-owned hardware and software configured to use a wireless connection for Internet access to FWS resources and intranet sites.

As the Federal Government and its employees take advantage of the benefits of teleworking (also known as telecommuting or flexiplace and travel), security presents new challenges. Offsite computers are highly mobile and inherently less controlled, and thus more vulnerable to security breaches that can impact the entire FWS network (now known as ESN, the Enterprise Services Network). The following set of wireless use security policies is designed to close these security gaps and make offsite wireless work a safer alternative for everyone involved.

**PURPOSE**

The purpose of this policy is to define security guidelines for use of FWS wireless internet connections that facilitate teleworking and traveling, and applies to all telework activities (core or situational telework, or travel). It establishes guidelines for appropriate use of FWS internal and external computing resources for employees (including volunteers and government-funded contractors), supervisors, and managers who participate in the Telework Program and use a wireless connection for Internet access.

This Wireless Use Policy does not replace existing security policies or directives associated with Telework. Rather, it supplements and further articulates existing security policies and practices, and provides Regional implementation of the Department's Wireless Use Policy, contained in a forthcoming Personnel Bulletin.

Failure to follow the R6 Wireless Use Policy 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, loss of telework opportunities, reassignment to other duties, demotion, suspension, termination, and possible criminal and/or civil prosecution.

**RESPONSIBILITIES**

In order to protect property and data assets, FWS has invested numerous resources to safeguard the enterprise (the network of computer systems) from threats to its sensitive data by securing its data centers, financial centers, and networks from hacking, malware, and other types of potential cyber-damage. Too often, though, the highly mobile laptop presents the greatest vulnerability to our resources, particularly by the uninformed, but well-intentioned, employee.

Federal employees and their managers are responsible for the security of Federal Government property and information, regardless of their work location. FWS and Region 6 security policies for telework and wireless use will be enforced at the same rigorous level when employees telework and travel, as when they are in the office.

**ALL EMPLOYEES:**

1. Must complete Wireless Security Awareness training, in addition to the mandatory DOI training requirements for IT Security Awareness, Privacy Act, and Records Management, and sign the R6 Statement of Responsibility/Liability (Attachment 3).
2. Must abide by the rules of appropriate wireless use as stated in this document, and the guidance contained in both the upcoming DOI Personnel Bulletin and RD's Order #5A-B.
3. Must abide by the following rules for appropriate and secure use of wireless connections:
  - DOI Virtual Private Network (VPN) is required for wireless use.
  - DOI VPN encrypts all data transmitted via wireless so no one can listen in.
  - You must start DOI VPN as soon as you establish a wireless connection.
  - DOI VPN must remain active throughout your entire wireless session.
  - You must turn off DOI VPN and terminate your wireless session when finished using the Internet.
  - The above requirements apply to wireless connections established anywhere.
4. Are responsible for the management and backup of information residing on their computer.
5. Employees who telework from home need to keep Government property and information safe, secure, and separated from their personal property and information.
6. Users need to be aware that all data and files residing on FWS equipment and infrastructure are subject to monitoring and inspection for security purposes. All data and files generated using FWS assets are the property of the Federal Government, and as such, no specific expectation of privacy or ownership should be expected.
7. Must represent the Service in a responsible manner in any Internet transaction.

**SUPERVISORS AND MANAGERS:**

1. Are responsible for knowing and enforcing the R6 Wireless Use Policy's rules for appropriate wireless use and protecting the Service's assets.
2. Are responsible for documenting the wireless telework arrangement in the form of a formal Telework Agreement (Attachment 1).
3. Are responsible for ensuring that the employee has completed and signed the Safety Checklist (Attachment 1).
4. Are responsible for providing the employee with a link to DOI Personnel Bulletin No. 05-02 on telework (<http://www.telework.gov/policies/DeptInteriorTeleworkPolicyA.pdf>), and a copy of RD's Order #5A-B.
5. Are responsible for ensuring that their employees receive proper Wireless Security Awareness training and have signed the R6 Statement of Responsibility/Liability (Attachment 3).

6. Are responsible for making the final determination as to the appropriateness of their employees' use of telework in order to meet management needs and mission objectives (i.e., position is conducive to telework, and employee has satisfactory performance appraisal).
7. Are responsible to notify the Office of IRTM 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.
8. In the event of a lost or stolen notebook computer, are responsible to notify both the IRTM Security Manager and the Board of Survey. Contact Tami Skinner, CGS Property Chief, for current Board of Survey rotation schedule.

**REGION 6 TECH SUPPORT HELP DESK:**

1. Is responsible for setting up notebook computers as defined in the guidelines (i.e., install and enable DOI VPN, BlueZone connection for FFS and FPPS/QuickTime, CompuSec encryption software, Cisco Security Agent intrusion prevention system, and Computrace's Lo-Jack software solution for protection and recovery).
2. Is responsible for setting up notebook computers with current operating system software and up-to-date patches, and security software (anti-virus) enabled. Notebook computers must be configured with the FWS standard image, personal firewalls enabled, be Windows XP STIG compliant, have encryption software enabled, and "least privilege" system settings applied, as practicable.
3. Is responsible for setting up designated wireless notebook computers to comply with the FWS Wireless Broadband 802.11x Access Security Technical Implementation Guide (STIG). Wireless capability is prohibited at all FWS facilities.
4. Conducts Wireless Security Awareness training sessions.
5. Provides notification that all network activities are subject to monitoring.
6. Repairs, updates, encrypts, etc., telework computers in the RO.
7. Requires that portable and mobile device access to organizational information systems be in accordance with organizational security policies and procedures, through only DOI-approved solutions.
8. IRTM does not have loaner notebooks for Telework.