

**U.S. FISH AND WILDLIFE SERVICE -- REGION 6****STATEMENT OF RESPONSIBILITY / LIABILITY****TELEWORK GUIDELINES**

Region 6 security measures cover all aspects of the information systems used by the teleworking employee, including paper and electronic files, other media, storage devices, and telecommunications equipment; e.g., laptops, PDAs, Blackberries, and cell phones. Employees who telework from home need to keep Government property and information safe, secure, and separate from their personal property and information. The following comprehensive security measures and appropriate uses will be followed by all employees engaged in telework. Employee liability for damages caused by failure to observe these practices is described.

**PHYSICAL SECURITY**

The laptop computer (also called a notebook) has become a particular hazard to protected data held by the Government and one that cannot be controlled solely by the use of firewalls and network access protocols. Physical security from loss, theft or damage is the single most important protection that a teleworker can apply to protect FWS hardware and information assets.

- Security cables will be supplied with each laptop to tie down the computer to a desk or other heavy object.
- Computrace's software solution Lo-Jack will cause stolen portable computers to "call home" (RO IRTM) when connected to the Internet and allow for geographic location for recovery.
- Never leave the computer unattended, even briefly, in any public place. Don't leave the computer in your hotel room, or if you must, secure it to an immovable piece of furniture with a cable lock.
- Select a carrying case that doesn't scream "computer inside!" Avoid cases with the computer manufacturer's name, logo, etc. Instead, use a regular briefcase with internal storage for the portable computer.
- Portable media, such as external disk drives, removable media, thumb drives, PDAs, etc., must be encrypted and are also governed by this security policy.
- Never leave computer equipment or peripherals visible on the seat of your car, even to run a "quick" errand. Always store it out of sight in the locked trunk when commuting to and from work or another destination.
- Do not let your notebook out of sight at airport security checkpoints.
- Use the notebook cable lock to secure your laptop at all times. Otherwise, you may be liable if it is lost or stolen.

**DATA SECURITY**

The loss or alteration of certain data, or its exposure to unauthorized persons, can damage FWS and, in many cases, other organizations or individuals as well. It is the employee's responsibility to protect the integrity of FWS data on an offsite computer.

- **Only a Government-provided notebook may be used for telework or travel. No personal equipment is to be used.**
- No other member of the household may use the Government computer.
- It is the employee's responsibility to ensure that others do not use the VPN account.
- The notebook must be used only for official Government purposes.
- Teleworkers must sign this Statement of Responsibility/Liability acknowledging that they understand the telework rules.

- Any teleworker using FFS or FPPS/QuickTime must not copy any of that information locally to the computer's hard disk, and the systems must only be accessed via secure VPN connection.
- Screen shots of sensitive information, particularly in FFS or FPPS/QuickTime, are not permitted at the telework site.
- FWS data may be stored/transported on memory sticks, which must be encrypted.
- Offsite password and access policies are the same as onsite security policies. Requirements for secure passwords (password length and complexity, avoidance of dictionary words and commonly used or easily guessed passwords, etc.), changing passwords on a regular basis, and prohibitions on divulging passwords or writing them down remain the same.
- While employees will not have access to network drives, access permissions and user rights will remain the same when employees telecommute, as notebooks will connect to the network when the employee is in the RO.
- Employees are responsible for backing up any data on the computers, and ensuring security of data being carried back and forth, whether on notebook computers or jump drives (memory sticks). It is strongly recommended that employees back up their laptops and jump drives on the office network, to preclude potential problems caused by loss or expiration of password, thereby making usage impossible on an encrypted device.
- Back up your data before you leave. Always back up your notebook before you do any extended traveling that may put your data at risk.
- When no longer needed, delete data from where it is stored.

#### **SOFTWARE AND NETWORK SECURITY**

Unauthorized software is prohibited and users must comply with software licensing requirements. Failure to comply with security practices can affect the entire ESN/FWS network, to which all FWS users connect.

All computers used offsite must be configured by IRTM according to FWS wireless guidance, including:

- Encryption of the Hard Disk
- Location Aware Firewall and Intrusion Detection system
- DOI VPN Client (required for all wireless usage)
- Disabling of wireless radio when on a wired connection
- Anti-virus software
- Lo-Jack
- BlueZone

The employee will not tamper with or disable any of the above.

- Software is governed by license rights. Only supported software is to be installed on the computer. Personal software, copied software, shareware, and vendor or free software from the Internet are prohibited, unless approved by IRTM.
- Users must remain vigilant about the risks of viruses and other "malware." Do not open suspect email attachments or click on suspect links.
- Only Notes email and iNotes may be used for official email purposes. Never send FWS work to a telework site (or any other destination) using a hotmail, yahoo, gmail, or other private email account.
- Do not send any sensitive information using an Internet email address (username @ example.com). Any email message sent with an Internet address is sent in clear text (unencrypted text) over the Internet.

- Windows XP software patches and updates will be set to automatically download and the employee is responsible for installing them.
- Any needed hardware or software repair will require the laptop be brought into the RO.
- Some configuration changes may be managed by IRTM through remote access. Other changes/updates/software installs will require the laptop be brought into the RO.
- The security posture of laptops will be monitored by IRTM staff by remote control sessions.
- Employees need to contact the R6 Tech Support Hotline (303-236-7926) if a security problem is discovered; i.e., if a virus or apparent unauthorized access is suspected.

#### **APPROPRIATE USE OF FWS EQUIPMENT OFFSITE**

The same rules of behavior governing equipment use in the RO apply to the telework site. Please review the R6 Rules of Behavior for Network Resources (Attachment 2).

- Home computers and equipment are not permitted for telework use.
- Only standard FWS software, installed by IRTM, may be used.
- FWS computing resources are not to be used by anyone except the FWS employee.
- FWS computing resources are to be used in support of FWS interests and not for any personal gain, business activities, charitable activities, or promotion of personal, political, or religious activities or beliefs.
- Email is subject to monitoring and cannot be guaranteed to be a private communication, especially when sent over the Internet.
- Email messages or other activities that suggest pornography, gaming, racism, sexism, offensive language, chain letters, streaming broadcasts (like Internet radio or weather, stock information, etc.) are prohibited. FWS has the right to access such information without giving notice to the user.

#### **POLICIES GOVERNING HIGH-SENSITIVITY WORK**

- Because of greater risks associated with the transport of data for telework, it is strongly recommended that FFS and FPPS/QuickTime work be conducted only at the RO site and not from the telework site.
- Screen-shots of sensitive data may not be used at the telework site.

#### **LIABILITY AND REPORTING REQUIREMENTS**

Each user is responsible for complying with this policy and is responsible for the notebook, peripheral equipment, and data in his/her care. If the teleworker or traveler does not use the cable lock to secure the laptop computer, and it is lost or stolen, then that person is liable for the entire replacement cost of the computer (not the amortized cost normally imposed by the R6 Board of Survey). The liability cost for lost, stolen, or damaged FWS data/information will be determined by the FWS Identity Theft Task Force and the Departmental CIO. The Regional IT Security Manager is required to report these issues through the Department's Computer Incident Response Capability, which includes notification of law enforcement.

#### **CONTACTS**

- Questions concerning the Board of Survey can be directed to Elliott Sutta, ARD-BA (303-236-3662), or Tami Skinner, CGS Property Chief (303-236-4325).
- Questions concerning the FWS Identity Theft Task Force and Department's Computer Incident Response Capability can be directed to Margaret Wolf, Regional IT Security Manager (303-236-8116).

**AGENCY COMMITMENTS:**

If the supervisor/manager approves a telework request from an employee, the Government will furnish/provide the employee with the following:

- Notebook/laptop computer which will be configured by IRTM with CompuSec encryption software, BlueZone connection for FFS and FPPS/QuickTime, enabled for wireless and DOI VPN, Cisco Security Agent intrusion prevention system, and Computrace's Lo-Jack software solution for protection and recovery.
- Locking security cable for immobilizing equipment at home or on travel.
- Payment of monthly utility cost (up to \$15/month) for providing high-speed Internet access if teleworking at least 2 days a week.

**EMPLOYEE COMMITMENTS:**

**I have read and understand this Statement of Responsibility/Liability governing my use of the R6 FWS IT and communications equipment and FWS data that facilitates my telework and travel activities, and agree to abide by both the R6 Telework Policy and R6 Wireless Use Policy. I understand that failure to do so may result in disciplinary action being brought against me.**

**I hereby certify that my Internet service connection for which I am requesting reimbursement has been used solely for official purposes (included "limited personal use" as allowed by Federal policy).**

**I hereby certify that I have taken the R6 Wireless Use training course via DOI Learn.**

**I understand that I may be liable for the full cost of replacing a lost or stolen computer if the locking cable was not used properly while working offsite.**

User Name (Please Print) \_\_\_\_\_

User Signature \_\_\_\_\_

Organization \_\_\_\_\_

Supervisor/Manager \_\_\_\_\_

Date \_\_\_\_\_