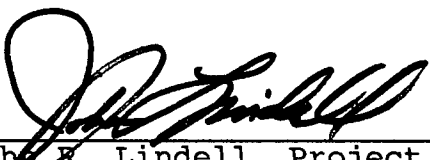


RCR
800.150

ADP SECURITY PLAN

Rice Lake National Wildlife Refuge
McGregor, Minnesota



John R. Lindell, Project Leader

9/26/89

Date

Statement of Purpose

This "ADP Security Plan" established the policies and procedures to protect the integrity of computer-based resources at this site. Specifically, the purpose of this plan is to:

- (1) Insure the confidentiality and integrity of ADP-based information resources; and,
- (2) Prevent damage or loss to ADP resources.

Statement of Policies and Procedures

The following policies are hereby established for ADP operations at this site:

1. Computer security is the responsibility of all employees who have access to Service computer systems. The Project Leader insures that all policies and procedures pertaining to ADP systems are documented and complied within an effective and efficient manner. All employees shall follow the ADP Security Plan and exercise reasonable precautions in the operation of all Service and Service-related ADP resources.
2. Computer resources are to be used for official Service business only. The Project Leader shall determine authorized use. Employees who intentionally misuse Service property (including computer resources and/or computer generated information) shall be subject to disciplinary action, reimbursement to the Government for the cost of the resources misused, and may face criminal prosecution.
3. ADP security is an ongoing process.

Additional policy and procedural components of the "ADP Security Plan" for this site are as follows:

- I. **Physical Security (Protection from Theft or Unauthorized Use)**
 - A. Microcomputer systems and other ADP components shall be physically secured during nonbusiness hours and when they are left unattended for extended periods of time. If a computer system cannot be protected behind a locked door, a theft deterrent device such as an "anchor pad," locking cabinet, locking cables, or other similar items shall be used to deter theft.
 - B. Computers that must be removed from the field station and taken to other Service offices, conferences, meetings, or the employee's residence must be accounted for. A property pass must be issued for any computer system or peripheral device that is removed from the site.

- C. All accountable computer resources must be accounted for upon transfer or termination of an employee with access to Service computer resources (or upon termination of a computer-related vendor contract).

II. Software Protection

- A. All computer software and data files must have backups! Duplicates of computer storage media (e.g. diskettes, hard disks, and tapes) containing programs and data files, provide for easier and less costly reconstruction in the event that the original is lost or damaged.
- B. All computer programs, data files, documentation, and storage media must be given to the Project Leader and accounted for upon transfer (or upon termination of a computer-related vendor contract).

III. Protection of Computer-Based Information (Data Integrity):

- A. Computer-based data such as proprietary information subject to the Privacy Act, or sensitive information, shall be protected to the same degree as if the information were on paper or micrographics. Usually, this means locking the storage media, printed copies, and documentation, in an approved security container when the storage media are not in use and the office is unattended. Storage media must be purged of all information by overwriting or reformatting before release for another purpose. Special procedures will be developed and implemented for information that is determined to be "sensitive" or "classified".
- B. Whenever passwords are used, they must be protected from disclosure and changed as needed. Passwords shall be changed with the departure of employees having access to existing passwords. Passwords should be easy to remember yet difficult for unauthorized persons to guess. Protect user password.
- C. It is important to protect passwords when Service computer resources are connected to larger "host" computer systems (usually in the mode of terminal emulation). Unauthorized disclosure of the user passwords compromises the security of the "host" computer and may result in major liabilities against the Service.
- D. Computer resources connected to answering modems should not contain proprietary information while unattended. Critical files and programs shall be "write" protected, and/or "pass-word" protected, whenever possible to avoid accidental or malicious damage or destruction.

IV. Computer Equipment/Software Property Accountability:

- A. Employees shall follow Service and Regional procedures and requirements regarding property accountability.** The Project Leader shall determine that all computer equipment, accountable software, application programs, data files and documentation are accounted for prior to changes in field station personnel.
- B. The "Local Support Person" shall maintain an Inventory of all computer resources located onsite** (or within the responsibility of the Project Leader). The inventory shall contain information concerning station computer(s), computer peripherals, all software, and major data files. The inventory shall reference all options or enhancements to each computer system located at the site. All software packages and routines, whether purchased or developed by the Government, shall be listed. All major data bases, and all critical and sensitive data bases, shall be contained in the station ADP inventory.
- C. The "Local Support Person" shall maintain a Software Documentation File.** The Software Documentation File shall include: a copy of the software agreement, a record of the registration, the serial number of the product, the date the software was received, a record of the Service property number assigned to the software package, and a record of software updates.

V. Copying Computer Software:

- A. Make copies only for security/backup purposes.** The reproduction of software for unauthorized use, or in violation of the licensing agreements, is illegal.
- B. Use the software on only one computer at a time** (unless specifically authorized to the contrary). If use on another computer is required, the Government must usually procure another copy of the software.

(Note: The majority of the computer software obtained for use by the Service is licensed and/or copyrighted for use on a single computer. The limitations regarding use of computer software packages, however, varies among vendors. Users are cautioned to carefully review the licensing agreement and documentation that accompanies the software.)

- C. Confidentiality of proprietary information and software must be maintained.** Anyone making unauthorized copies of proprietary information or software shall be subject to disciplinary action and may be subject to criminal prosecution or civil suit.

- D. Backup copies of newly acquired software should be made as soon as possible. The end user and the Project Leader are jointly responsible for insuring that timely backup copies of software and data are made and stored in an appropriate location.

VI. Physical Security (Environmental Protection):

- A. Procedures shall be taken to provide environmental protection for all computer equipment, software, computer-based data, and other computer resources under the authority of the Project Leader at this site. This shall include, but is not limited to, the following concerns: adequate environmental controls (e.g., air temperature, air quality, and relative humidity), maintenance of ventilation clearances, and appropriate protection from power fluctuations and lightening strikes.

ADP Security is an ongoing responsibility. Taking ordinary and reasonable precautions against loss or damage of ADP resources is the responsibility of all Service employees. This includes managers, Project Leaders, information systems professionals, and especially - members of the user community.