Reclamation Manual

Directives and Standards

Subject: Reclamation Information Technology (IT) Security Program (ITSP): System Backup Requirements

Purpose: Specifies Reclamation's backup and recovery requirements for all IT systems.

Authority: The Privacy Act of 1974 (5 U.S.C. § 552a); Federal Managers' Financial Integrity Act of 1983 (Public Law 97-255); The Computer Security Act of 1987 (Public Law 100-235); Fiscal Year 2001 Defense Authorization Act (Public Law 106-398), Subtitle G, *Government Information Security Reform*; Office of Management and Budget (OMB) Circular No. A-130, Appendix III, *Security of Federal Automated Information Systems* (50 Federal Register 52730, December 24, 1985); OMB Circular No. A-123, *Management Accountability and Control* (31 U.S.C. § 3512, June 21, 1995); *Practices for Securing Critical Information Assets*, Critical Infrastructure Assurance Office (CIAO) (January 2000); Department of the Interior Departmental Manual Part 375, Chapter 19, *Information Technology Security*.

Contact: Information Resources Services, D-7100

1. **Introduction.** This Directive and Standard establishes Reclamation's backup and recovery processes and archival storage and disposal requirements for electronic data and software.

2. **Goals.** The goal of this Directive and Standard is to enable IT system recovery and operation in case of data and/or software loss or corruption. The ability to recover data and software limits productivity loss.

3. **Definitions.**

   A. **Backup.** The process of copying data from systems/computers working storage to a transportable electronic media such as magnetic tape, laser or magnetic disks, etc. Backups may include selected computer files or entire systems of data with operating and control files and scripts.

   B. **Archival.** The storage of transportable electronic media in a permanent or temporary storage location.

   C. **Disposal.** Prescribed destruction methods for electronically stored data dependant upon the highest level of sensitivity of the data.

   D. **Recovery.** Restoring data to an operational system/computer from a previously copied set of data from its portable storage media.

   E. **Server.** Any computer simultaneously used or accessed by more than one user or automated system. Computers used for dependent or independent controls are also

considered servers when data is collected and/or stored, e.g., Supervisory Control and Data Acquisition Systems (SCADA) "master station."

F. **Continuity of Operations (COO) Plans.** Plans that facilitate the restoration and performance of essential functions during any emergency or situation that may disrupt normal operations.

4. **Scope.** This Directive and Standard applies to:

A. All Reclamation-owned, -operated, and -maintained IT systems, including specialized systems [e.g., SCADA, Hydromet, Geographic Information Systesms (GIS), Dam Safety].

B. All Reclamation-owned IT systems operated and/or maintained by contract or temporary personnel.

C. All Reclamation-owned IT systems operated and/or maintained by organizations or personnel other than Reclamation.

5. **Procedures.**

A. **Backup Requirements.**

(1) **Server Backups.**

(a) A server's entire system will be backed up weekly (for operating system software, data, control files, etc.) and daily (for files changed or added). It may be impractical to backup data on systems where data are constantly changing (e.g., data in SCADA systems, satellite imagery, etc.); however, for these systems, the system software, applications, and control files will be backed up monthly and as changes occur. All exceptions will be approved by the Office/Regional Director or his/her delegate. Backup schedules and storage sites are to be approved by the Regional Information Technology Security Manager (ITSM). The approved documented schedule will be stored at the operational site with a copy to the ITSM.

(b) Storage of weekly/monthly backup media will comply with the Archival Storage requirements in paragraph 5B.

(c) Daily backup tapes/disks may be recycled in 7- or 14-day increments. Weekly backup tapes/disks will be recycled every month. Monthly backup tapes/disks will be stored for 120 days, minimally, before recycling or destruction.

(d) Transportation of storage media to and from the archival storage location must be performed by a trained, trusted, Reclamation employee or bonded, trusted couriers.

(2) **Continuity of Operations Plan.** Backup procedures will be incorporated into system and facility COO Plans.

(3) **Desktop/Portable Backups.** Users are responsible for the backup of data stored on their assigned personal computer's and/or workstations. Weekly backups are recommended. Permanent backup storage media on users' computers such as a streaming tape drive or a large portable disk (e.g., "ZIP Drive") are permitted for data not considered Reclamation restricted or sensitive. All users will ensure job-critical data, excluding user's software, are backed up on their local area network (LAN) server. LAN servers will have adequate disk storage to backup all users' job-critical data files. A user may use a different desktop backup procedure if approved by the ITSM in writing.

(4) **Labeling.** All backup media will be labeled with the date of the backup, type of backup, and highest data sensitivity that may be found on the media. See the Information/Data Security Directive and Standard for guidance on data sensitivity.

B. **Archival Storage.**

(1) Archival storage locations must be at least 1 mile away (usually 3 miles or more), and/or not likely to be affected by the same natural disasters such as flooding, earthquakes, and fire as the processing site. Storage locations must be environmentally protected to preserve data media, and access controlled. Data considered Reclamation restricted or sensitive should be stored in an encrypted format, preventing disclosure in the event of theft. The encryption method should be machine independent (e.g., encryption keys not unique to the machine that created the data). When a portion of the data stored on a medium must be encrypted, it is recommended that the entire disk/tape be encrypted.

(2) Long-term storage data, in excess of 90 days, including monthly backups, must be written on media designated secure for long-term storage. Used magnetic media will not be used for long-term storage. Write-once CD-ROM can be used for long-term storage. Storage media will be erased, cleaned, and certified as safe before being reused for short-term storage.

(3) Archival storage procedures will be incorporated into system and facility COO Plans. A copy of COO Plans will be stored at the archival storage location.

C. **Recovery of Data.**

(1) Necessary steps will be taken to verify all data on the media can be restored. Backup data will be recoverable from the prior weekly backup plus incremental daily backups as needed.

(2) Systems considered non-critical and typically not used over weekends and holidays will be recoverable from the prior working day.

(3) Recovery procedures will be incorporated into system and facility COO Plans.

(4) Recovery procedures will be tested annually.

6. **Responsibilities.**

A. **Chief Information Officer (CIO).** The CIO has overall responsibility for the ITSP in Reclamation.

B **Directors of Reclamation Regions and Offices.** Directors of Reclamation Regions and Offices have responsibility for the security of the IT systems under their authority. This responsibility may be delegated no more than one level down (Deputy or Assistant Directors).

C. **Information Technology Security Managers (ITSMs).** ITSMs coordinate and verify backup, archival, and recovery procedures are adequate and support the Reclamation-wide IT security policy and Directives and Standards.

D. **System Administrators (SAs).** SAs have the responsibility to develop system specific backup and recovery procedures and to ensure prescribed backups take place as described in this Directive and Standard. SAs also ensure that backup media is properly stored and disposed of pursuant to the processes described in this Directive and Standard.

E. **Users.** Users are responsible for supporting systems backup procedures and ensuring those systems and data for which they are directly responsible are protected through backup procedures described or inferred through this Directive and Standard.

7. **Related Directives and Standards.** For related and supporting Directives and Standards see the Information Resources Management (IRM) section of the Reclamation Manual.