Reclamation Manual
Directives and Standards

Subject: Reclamation Information Technology (IT) Security Program (ITSP): Acceptable Use of Government-owned IT

Purpose: Establishes users' responsibilities for acceptable use of Reclamation IT.

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) Title X, Subtitle G, *Government Information Security Reform*; Office of Management and Budget (OMB) Circular No. A-123, *Management Accountability and Control* (31 U.S.C. § 3512, June 21, 1995); OMB Circular A-130, Appendix III, *Security of Federal Automated Information Systems* (50 Federal Register 52730, December 24, 1985); National Institute of Standards and Technology; Department of the Interior Departmental Manual (DM) Part 375, Chapter 19, *Information Technology Security*; DM Part 377, *Telecommunications*; and DM Part 410, Chapter 2, *Limited Personal Use of Government Equipment and Library Collections*

Contact: Chief, Information Office, D-2200

1. **Introduction.** Computer use is a major aspect of nearly every Reclamation employee's and contractor's work. In order to provide for adequate security and to protect Reclamation, precautions and limits on the use of Government-owned IT must be established.

2. **Goal.** The goal of this Directive and Standard is to provide the policy necessary to ensure that Reclamation computer users follow established rules and guidelines for the acceptable use of IT equipment.

3. **Scope.** This Directive and Standard applies to all Reclamation employees, contractors, consultants, and volunteers, including those personnel affiliated with third parties who access Reclamation internal networks.

4. **Procedures.**

   A **Gaining Access to Reclamation Systems.** All users of Reclamation IT equipment and systems must be granted access through established procedures prior to using Reclamation IT systems or equipment. System administrators, system managers, system owners, system security officers, and users may not grant access to Reclamation IT systems to anyone without following established procedures. Contact your local help desk for procedural information.

Reclamation Manual
Directives and Standards

B. **Rules of Behavior.** Every user is responsible for reading and complying with the *Bureau of Reclamation – General Rules of Behavior for Use of IT Systems and Equipment*. Users of special applications such as Supervisory Control and Data Acquisition Systems, personnel systems, or financial systems must follow any additional rules of behavior for those systems.

C. **Data Protection.** Users are responsible for understanding the data classifications for data stored and transmitted on Reclamation IT systems. Users are also responsible for following established guidelines for the protection of data transmitted and stored on Reclamation IT systems. See Reclamation Manual, *Information/Data Security,* IRM 08-11, for additional information.

D. **Desktop Computer Protection.** "Common Sense" care of computer hardware equipment must always be exercised by the user. Desktop personal computers and workstations will be kept within a secured area. Reclamation employees and contractors will follow reasonable measures to protect against theft, vandalism, or access by unauthorized users. If theft of equipment seems likely, the equipment must also be physically secured to the furniture by cables, bolts, or other approved methods.

E. **Portable Computer Protection.** Users will protect portable computers and devices assigned to them from theft, misuse, and damage.

F. **Shared Workstations.** The designated custodian of shared workstations is responsible for ensuring compliance with applicable IT security Policy and Directives and Standards.

5. **Responsibilities.**

A. **Chief Information Officer.** The Chief Information Officer has overall responsibility for the ITSP.

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. **Reclamation Managers/Supervisors/Custodians.** Reclamation Managers/ Supervisors/Custodians have responsibility for assuring compliance to this Directive and Standard by their employees and contractors.

D. **Reclamation Employees.** Reclamation employees are responsible for compliance with ITSP Directives and Standards, and those who willingly and deliberately violate them will be subject to disciplinary action.

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