



# United States Department of the Interior



BUREAU OF RECLAMATION  
Great Plains Region  
P.O. Box 36900  
Billings, Montana 59107-6900  
April 2, 2007

IN REPLY REFER TO:  
GP-1220  
ADM-1.00

VIA ELECTRONIC MAIL ONLY

## MEMORANDUM

To: All Employees, Great Plains Region

From: Michael J. Ryan /s/ Gary W. Campbell  
Regional Director

Subject: Appropriate Use of the Internet

I would like to remind employees of their responsibility to ensure the Internet is used for its intended and permitted purpose. Employees can learn about their Internet responsibilities by reading the Reclamation Manual CMP PO2 and CMP 03-01. For a quick reference the following Internet activities are strictly prohibited using government equipment and time:

- Gambling
- Viewing/downloading sexually explicit material
- Lobbying Congress or any government agency (unless as required as part of your official duties under applicable statutory authority and bureau policy)
- Commercial activities, including purchases for commercial gain, such as day trading (securities) and outside work
- Endorsement of any outside products, services or organizations
- Live streaming or video streaming music, images, or information

Employees should have no expectation of privacy when using the Internet during work hours. All activity to and from the Internet is logged and monitored by the Department.

Recent reviews of employee Internet use conducted by the Inspector General and the Chief, Information Officer, showed a number of employees are violating Departmental policy. Some of these activities have significant legal and administrative consequences, up to and including dismissal from employment. Violators may also be subject to criminal charges.

Please take the time to familiarize yourself with Departmental and Reclamation policy. Your full cooperation in complying with these regulations is important to you and to Reclamation.



# United States Department of the Interior

BUREAU OF RECLAMATION  
P.O. Box 25007  
Denver, Colorado 80225-0007

IN REPLY REFER TO:

**MAR 31 2011**

84-21000  
IRM-1.10

VIA ELECTRONIC MAIL ONLY

## MEMORANDUM

To: All Bureau of Reclamation Employees

From: Bruce C. Muller, Jr.   
Acting Director, Chief Information Office

Subject: Adoption of the Bureau of Reclamation Rules of Behavior

To promote generally accepted practices with concern to the appropriate and limited use of government-furnished Information Technology (IT) resources, Reclamation is hereby adopting the attached updated Rules of Behavior (ROB), dated March 18, 2011. These rules apply to all Reclamation computer users, whether federally employed or contracted.

This ROB documents the baseline requirements for all users of Reclamation IT systems and addresses the efficient, ethical, and lawful use of government-provided IT or government-furnished equipment (GFE), including, but not limited to, workstations, hand-held devices (for example, Personal Digital Assistants and Smartphones), laptop computers, servers, printers, copiers, networks, and network equipment, owned or leased by Reclamation.

The following list identifies a few of the significant changes made to the original document:

- Users are allowed to access Department of the Interior approved Social Media sites.
- All sensitive information as defined by Reclamation Directive and Standard (D&S) SLE 02-01 *Identifying and Safeguarding FOR OFFICIAL USE ONLY (FOUO) Information*, while maintained on mobile media (CD/DVD, thumb drives, laptops, Smartphone, etc.) will be encrypted while being transported outside of Reclamation facilities or when transmitted outside of the Department electronic environment.
- Guidance from the Department IT Security Handbook states any remote access to a Department network will be initiated from GFE only and will use an agency or bureau approved secure communication channel, such as the Virtual Private Network or Secure Socket Layer. As an exception to this rule, the Office of the Chief Information Officer has formally accepted the risk associated with the use of Outlook Web Access to view bureau email from any device, including hand-held devices.

In an effort to meet this guidance:

- Training will be provided to educate on the risks that are associated with not utilizing GFE.
- Options for ensuring that users who are required to access bureau systems remotely have GFE: (this could include users who travel or work from home)
  - Obtain a “loaner” laptop from your local service center
  - As systems are retired, replace them with docking station laptops (Reclamation D&S IRM 08-18 *Personal Computer (PC) Life Cycle Management*)
- New users will be required to sign the new ROB, current employees will be required to read and acknowledge the ROB as part of the annual Federal Information System Security Awareness Training.

If you have any questions concerning these general ROB, please contact Mr. Ben Weinischke, Bureau Chief Information Security Officer, at 303-445-2911.

Attachment

Distribution E

## General Information

### Application

These general Rules of Behavior (ROB) apply to all Reclamation computer users, whether federally employed or contracted. This ROB is to be read and individually acknowledged by all users of Reclamation computer systems.

### Purpose

This ROB document serves as a baseline requirement for users of all Reclamation IT Systems. This document is intended to address the efficient, ethical, and lawful use of government provided information technology, also defined as government furnished equipment (GFE), including workstations, handheld devices (e.g., personal digital assistants (PDAs), smart phones, blackberries, etc.), laptop computers, servers, printers, copiers, networks, and network equipment, owned or leased by Reclamation. Systems with special security requirements may establish additional rules of behavior to supplement those established herein.

### Authority

This ROB has been prepared to address the requirements of the *Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resource, Department of the Interior IT Security Policy* and the *National Institute of Standards and Technology (NIST) Special Publication 800-53, Recommended Security Controls for Federal Information Systems, Appendix F, Control Family Planning, Control PL-4 Rules of Behavior*.

### Revisions

**Summary of Revisions** - This revision to Reclamation's *Rules of Behavior for Use of IT Systems and Equipment*, dated March 18, 2011, incorporates changes necessary under departmental guidance, NIST guidance, and as a result of revisions and changes to Reclamation's own Directives and Standards (D&S). The bulk of the changes support improved protection of Personal Identifiable Information (PII), enhanced remote access procedures, use of social media Web sites and established a requirement that users now review and acknowledge the ROB as part of the annual Federal Information Systems Security and Awareness (FISSA) training.

Title:

**Bureau of Reclamation – General Rules of Behavior for Use of IT  
Systems and Equipment**

Date:

**3/18/11**

**Applicability of Prior Versions** – Prior versions of this document, even if signed in acknowledgement, do not meet present Department expectations. All IT resource users must read and acknowledge this revision to the ROB as part of their annual IT Security training.

**Table of Contents**

**Page**

1. REFERENCES.....4

2. RULES .....5

    2.1 GENERAL.....5

    2.2 TRAINING.....5

    2.3 ACCOUNT AND ACCESS CONTROL MANAGEMENT.....5

    2.4 PASSWORD MANAGEMENT .....6

    2.5 AUTHORIZED USE OF GOVERNMENT EQUIPMENT .....7

        2.5.1 Limited Personal Use of Government IT Equipment .....7

        2.5.2 Internet/Intranet.....8

        2.5.3 E-mail.....8

        2.5.4 Social Media Sites.....9

    2.6 IMPROPER USE OF GOVERNMENT IT EQUIPMENT.....9

    2.7 PROPER USE OF COPYRIGHTED MATERIALS.....10

    2.8 CONSEQUENCES OF BEHAVIOR INCONSISTENT WITH THESE RULES .....11

    2.9 ANTI-VIRUS AND ANTI-SPYWARE SOFTWARE.....11

    2.10 REPORTING OF IT SECURITY INCIDENTS.....11

    2.11 DISPOSAL OF IT ASSETS.....11

    2.12 HANDLING OF SENSITIVE INFORMATION .....12

    2.13 REMOTE ACCESS.....13

    2.14 BACKUP.....14

    2.15 PHYSICAL PROTECTION AND SECURITY.....14

    2.16 ASSIGNMENT AND LIMITATION OF SYSTEM PRIVILEGES.....14

    2.17 SYSTEM MONITORING .....15

    2.18 DEFINITIONS.....15

3. ACKNOWLEDGEMENT.....17

## 1. References

### **NIST Standards<sup>†</sup>**

*National Institute of Standards and Technology (NIST): Special Publication 800-53  
Recommended Security Controls for Federal Information Systems*

*National Institute of Standards and Technology (NIST): Special Publication 800-122  
Guide to Protecting the Confidentiality of Personally Identifiable Information PII*

### **OMB Requirements**

*Office of Management and Budget (OMB): Circular No. A-130, Appendix III, Security of  
Federal Automated Information Resources*

### **Departmental Requirements<sup>‡</sup>**

*Departmental Manual: Section 375 Chapter 19 Information Technology Security  
Program.*

*Departmental Manual: Section 410 Chapter 2 Limited Personal Use of Government  
Office Equipment and Library Collections.*

*Department of the Interior IT Security Policy*

### **Bureau of Reclamation Requirements<sup>§</sup>**

*Reclamation Manual: D&S SLE 02-01 Identifying and Safeguarding FOR OFFICIAL  
USE ONLY (FOUO) Information.*

---

<sup>†</sup> NIST Special Publication 800-53 can be found at: <http://csrc.nist.gov/publications/nistpubs/>

<sup>‡</sup> 375 DM 19 and 410 DM 2 can be found at: [http://elips.doi.gov/app\\_dm/](http://elips.doi.gov/app_dm/)

<sup>§</sup> A list of Reclamation's Directives and Standards can be found on the Reclamation Website at:  
<http://www.usbr.gov/recman/DandS.html>

## **2. Rules**

### **2.1 General**

These rules apply to all users of Reclamation IT equipment and systems, and in some instances, to the equipment and systems themselves. The purpose of this ROB is to provide the minimum acceptable standard for conduct associated with the use of Reclamation IT systems and equipment. Compliance with this ROB promotes the security of Reclamation's IT systems. The security of Reclamation's IT systems is a shared responsibility in which every user plays a key role.

Users are responsible for reading and abiding by the ROB pertaining to the use of Reclamation IT systems and equipment. Appropriate behavior is defined as activities generally considered suitable in a public environment. The applicable materials are listed in the *References* section of this ROB.

### **2.2 Training**

All new users of IT systems and GFE are required to complete security awareness training prior to gaining access to Reclamation IT systems or equipment. All users are required to take annual IT security awareness refresher training. Failure to complete such training in a timely manner will result in the revocation of access privileges. (Refer to section 2.8)

Those users that may have additional IT security responsibilities (refer to Section 2.16, *Assignment and Limitation of System Privileges*) will be required to complete annual supplemental "Role-based" IT security training. Although this training will be required for a specific IT system user and management community (refer to *Department Role-Based Security Training Standard*), a discussion of the details of the required training is beyond the scope of this document.

Note: For further information see: *Department IT Security Policy: Awareness Training (AT)*.

### **2.3 Account and Access Control Management**

Users shall only use accounts for which they are authorized. Users shall not divulge account access procedures or access information to any user not authorized access to that account.

Files are owned by specific accounts (i.e., users), and file sharing is controlled by file ownership and permissions set by the account user or System Administrator(s). Users shall not attempt to gain access to files to which they do not have ownership and/or permission.

All information stored on government-owned IT systems and equipment is the property of the government. A user is responsible for protecting and maintaining, to the best of his/her ability, any information used or stored in his/her accounts. A user shall not attempt to access any data or programs contained on systems for which he/she is not authorized or does not have explicit consent of the account manager or their supervisor.

When a user no longer requires access to IT resources, he/she will notify the appropriate supervisor, account manager, system administrator or Information System Security Officer (ISSO), and make no further attempt to access these resources.

The user will contact his/her supervisor, account owner, or system administrator for additional computing resources or privileges needed to access applications and data. The user will also contact his/her supervisor, account owner, or system administrator if they determine they have more privileges than necessary.

Although all systems must have a password-protected screen saver that activates after 15 minutes of inactivity, it is recommended that whenever a user leaves the computer unsupervised, the user should log-out of or manually lock their account. Note: Pressing the Windows Key and L or <CTRL-ALT-DEL> will lock the computer. When using the Department Access card, removal of the card from the reader will also lock the computer.

Note: For further information see: *Department IT Security Policy: Access Control (AC)*.

## **2.4 Password Management**

Passwords are required on all user accounts used to access government provided systems and applications. Passwords should not be commonly used words or names, and should not be easily guessable dictionary passwords. Your passwords must be comprised of alphanumeric characters (uppercase, lowercase, numeric, and special characters).

Users shall not share their passwords with others nor store passwords in locations or in forms that are readily accessible to others who do not have a specific need to know. This includes storing passwords in unencrypted word processing files, spreadsheets, and databases. Passwords shall be committed to memory whenever possible and shall not be written down except as necessary to enable emergency access to administrator accounts. Whenever written down, passwords shall be maintained in a physically secure location which is not in the same immediate vicinity as the computer(s) to which they apply.

Note: For further information see: *Department IT Security Policy: Identification and Authentication (IA)*.

## 2.5 Authorized Use of Government Equipment

Note: *This section is excerpted from Department IT Security Policy, Applicable use Security Standard, dated March 17, 2008.*

Government resources (e.g., computer equipment, networks) and electronic communication facilities (such as e-mail, Internet access, or Web applications) are for authorized government use only except as otherwise stated in this section.

The following limited personal uses of government IT equipment and systems are hereby authorized for all employees. Supervisors should be consulted prior to any personal use of government IT equipment if there is any question whether such use is appropriate under the terms of this ROB.

### 2.5.1 Limited Personal Use of Government IT Equipment

Users may use government IT equipment only for official business or as otherwise authorized by the Government. These rules authorize *limited personal use*\*\* of certain government IT equipment, as long as it occurs on *non-duty time*\*\*, does not interfere with official business, is not a *commercial gain activity*\*\* or is otherwise prohibited, and the expense to the government is *negligible*\*\*.

**Users on non-duty time** are allowed limited use of government IT equipment for personal uses that involve only negligible expense to the government (e.g., Internet usage as allowed by this ROB, sheets of paper, ink, and ordinary wear and tear) and do not interfere with official business. For purposes of these rules, IT equipment includes desktop computers, portable computers, servers, printers, personal digital assistants, and networks. Printers are for official business; however, personal use of less than ten pages per week is permissible on occasion.

Loading personally-owned software (such as tax preparation programs, computer games, etc.) on government machines is prohibited. Personal print jobs should be completed using black and white, where available. Use of color print jobs should be limited in quantity due to the high associated costs. Users may not use official stationery, envelopes, or postage for personal purposes under any circumstances. Use of any personally-owned (non-government furnished) equipment to connect or communicate with any Reclamation network or system is prohibited.

---

\*\* Reference: Definitions, Section 2.18 of this document

### **2.5.2 Internet/Intranet**

**Users on non-duty time** are allowed to use the Internet for personal use. However, specific care should be taken when visiting sites which may contain malicious code that may cause a disruption to Reclamation systems. All users must be aware that all Internet usage is logged and viewable by supervisors in the event that abnormal amounts of time are being spent on the Internet. Specific restrictions on personal use of the Internet are listed in the section of these rules entitled Improper Use of Government IT Equipment (Section 2.6).

### **2.5.3 E-mail**

**Users on non-duty time<sup>††</sup>** are allowed to use government e-mail systems and computers for limited personal use with the following restrictions:

The cost to the Government for the personal use of e-mail must be negligible. Personal use of e-mail also must not cause congestion, delay, or disruption of service to any government system or equipment; e.g., by transmitting large attachments.

Users may use e-mail for personal point-to-point electronic transmissions or personal transmissions not to exceed five addressees per e-mail, both as employee-generated personal messages and in response to personal messages received by the employee. The use of e-mail distribution lists or *Broadcast transmissions<sup>††</sup>* for personal use are prohibited unless specifically authorized.

Users using e-mail for personal purposes must not represent themselves as acting in an official capacity.

Automatic e-mail message forwarding is only permitted to authorized department e-mail accounts within the Department controlled e-mail environment; otherwise, an alternative secure method shall be employed when an addressee is unavailable to receive e-mail that is required to move business processes. E-mail containing information labeled sensitive – for official use only, controlled unclassified information, or classified is prohibited from being sent outside of the Department-controlled environment, unless the e-mail is encrypted.

---

<sup>††</sup> Reference: Definitions, Section 2.18 of this document

<sup>‡‡</sup> Reference: Definitions, Section 2.18 of this document

#### **2.5.4 Social Media Sites**

Users on non-duty time are allowed to use government resources to access social media sites which have been specifically allowed for Department users.

Unauthorized use of instant messaging to include online chat resources, unless specifically authorized by the users' supervisor is prohibited.

### **2.6 Improper Use of Government IT Equipment**

Unauthorized or improper use of government IT equipment could result in disciplinary or adverse personnel action (as described in the *Department Personnel Handbook* on Charges and Penalty Selection for Disciplinary and Adverse Actions), loss of or limitation of use of equipment, criminal penalties, and/or users being held financially liable for the cost of improper use.

Users are prohibited from using government IT equipment and e-mail for personal uses except as permitted by these rules or authorized by regional IT managers.

Users are prohibited from using government IT equipment, at any time, for activities that are illegal; e. g., gambling (5 CFR 735.201), or that are inappropriate or offensive to co-workers or the public, such as the use of sexually-explicit material, or material or remarks that ridicule others on the basis of race, creed, religion, color, sex, disability, age, national origin, or sexual orientation.

Users are prohibited from using government IT equipment at any time for any outside fundraising activity, endorsing any product or service, participating in any lobbying activity, or engaging in political activities. Note: different rules for lobbying and political activity apply to employees appointed by the President and confirmed by the Senate. Those employees should consult the Department Ethics Web site for guidance (<http://www.doi.gov/ethics/>.)

Users are prohibited from using government IT equipment at any time to make purchases for personal commercial gain activity.

Users are not authorized to remove government property from the office for personal use.

Users are prohibited from using government-provided access to the Internet to present their personal views in a way that would lead the public to interpret it as an official Government position. This includes posting to Social Media Web sites such as Facebook, YouTube, and Flickr, or other public forums while using a government account.

Users are prohibited at any time from using the Internet as a radio or music player. Such live stream use of the Internet could strain the Reclamation network and significantly slow communications, inhibiting Reclamation employees from conducting official business.

Users are prohibited at any time from using "push" technology on the Internet or other continuous data streams, unless they are directly associated with the employee's job. Push technology from the Internet means daily, hourly, or continuous updates via the Internet; e.g., news, stock quotes, weather, and similar information. Continuous data streams could degrade the performance of the entire network.

Users are prohibited at any time from using an Internet Service Provider to gain access to the Department e-mail system or for any other system operation or service without an approved and authenticated Virtual Private Network (VPN) connection utilizing an authorized username and password or Department Access Personal Identify Verification card. As an exception to this rule, the Department has formally accepted the risk of using Microsoft's Outlook Web Access (OWA) for accessing e-mail.

Users are prohibited at any time from using Internet peer-to-peer networking services on government computers.

Users are prohibited at any time from using government resources to construct or operate a personal Web page.

Except where and when specifically authorized, users are prohibited from loading and operating security tools such as network sniffers, vulnerability scanners, and exploit code. The use of these tools is restricted to personnel who understand the potential performance and security impacts and are authorized to perform security testing, evaluation, and/or monitoring.

## **2.7 Proper Use of Copyrighted Materials**

All copyrighted material (software, documents, or methods) shall be treated as sensitive information. This includes all software copies made for backup purposes. Disposal of all copyrighted material shall be in accordance with the copyright holder's requirements (per the license agreement) or other sensitive material disposal guidelines.

To the greatest extent practical, system administrators shall ensure that workstations and servers have valid software licenses for software deployed on the systems. To help support this, users shall not make or use unauthorized copies of copyrighted software, except as permitted by law or the owner of the copyright. No software shall be loaded onto systems or used except as permitted by law or by the owner of the copyright. All software shall be used in accordance with its license, instructions, and restrictions.

## **2.8 Consequences of Behavior Inconsistent with These Rules**

Behavior inconsistent with these rules will be handled by management officials who may enlist the assistance of system administrators and/or the Chief Information Security Officer (CISO) as appropriate. Violations may result in personnel actions being taken, depending on the severity of the situation. Users may have their access to IT resources further restricted or terminated, if such activities are warranted. Failure to abide by Department, Reclamation, local division/office, or system policies may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

## **2.9 Anti-virus and Anti-spyware Software**

Various anti-virus and anti-spyware software systems and programs are used throughout Reclamation. Users are responsible for maintaining the integrity of portable computers or computers that are infrequently attached to the Bureau network and are used for remote access to Reclamation systems by employing approved anti-virus and anti-spyware software and keeping virus and spyware definition files up to date.

Users shall not modify or disable, or cause the disruption of, anti-virus and anti-spyware software protections without the prior authorization of the system owner or the Regional Information System Security Manager (RISSM).

Note: For further information see: *Department IT Security Policy: System and Information Integrity (SI)*.

## **2.10 Reporting of IT Security Incidents**

Users are required to immediately report any and all observed compromises of security (viruses, unauthorized access, theft, inappropriate use etc.) to the appropriate person as stated on the Reclamation Incident Handling Capability intranet site <http://intra.do.usbr.gov/usbrit/Security/incidnt/Incident.html>. Wherever practical, reporting should occur personally or via telephone to avoid the possibility of incident information being compromised in any way.

## **2.11 Disposal of IT Assets**

Sensitive information (including copyrighted software, personnel information, proprietary scientific data, and remote access applications) is to be removed from hardware devices prior to removal from service, or prior to transferring ownership of those devices unless the information/software is specifically included in the transfer. Users must follow the current *IT Asset Disposal D&S – IRM 08-13*, for information sanitization prior to the disposal or transfer of government IT assets.

Note: For further information see: *Department IT Security Policy: System and Information Integrity (SI)*.

## 2.12 Handling of Sensitive Information

Users are responsible for understanding and complying with the handling and protection requirements of any data they use or create. When in doubt, users should consult their respective manager/supervisor.

Reclamation users are responsible for protecting sensitive information (including For Official Use Only, Privacy Act, and PII) to which they have access. All such information shall be protected from unauthorized access or disclosure in accordance with the applicable handling requirements for that information.

Wherever practical, sensitive information is to be removed by users from any systems before they are sent out for repair. Where sensitive information cannot be removed from devices requiring repair, users should work with local IT Operations, IT Security, and Acquisitions staff to ensure that the repair services are procured from trusted and confidential resources.

When no longer needed, paper copies of sensitive information are to be shredded and sensitive information on external writeable media (i.e. CD/DVD disks, thumb drives, etc.) is to be erased. External media including hard drives, other electronic devices, or documents with sensitive information are to be stored in locked containers when not in use or when you leave your work area. All media, including diskettes, external hard drives/devices or documents containing sensitive information should be clearly labeled as such.

Users must encrypt all sensitive and PII information electronically stored on any equipment, including, but not limited to, computers, portable hard-drives, PDAs, and thumb drives, any time the equipment is outside of Reclamation facilities, or when the information is transmitted outside of the Department, including sensitive and PII information downloaded to computer systems accessing that information via remote access (see Section 2.13). Note: contact the Reclamation Enterprise Services Center (RESC) for assistance with installation and usage of Reclamation approved encryption tools.

No part of this ROB is intended to address the specific handling or protection of information at a classified, law enforcement sensitive, confidential or other information classification level. ROB for IT systems storing, processing, or communicating these information types must address these requirements as a part of their security protection plan.

Note: For further information see: *Reclamation Manual: D&S SLE 02-01 Identifying and Safeguarding FOR OFFICIAL USE ONLY (FOUO) Information.*

### 2.13 Remote Access

Access to Department or Reclamation IT resources from a location not under the direct control of the Department or Reclamation is considered “remote access.” Personnel using remote access to gain admission to Reclamation’s IT resources will abide by this ROB. The user will use all remote access equipment in accordance with established acceptable use restrictions and procedures, as addressed in this document. All remote access connections made to Department or Reclamation IT networks or systems will be made through the agency or Bureau approved VPN (or similar secure communication channel) using GFE. In the event of a contingency or disaster event the Reclamation Authorizing Official may allow temporary use of non-GFE to access Reclamation IT resources and/or networks. This remote access will be authorized for specific users and time periods.

Users working away from their official duty station must use authorized procedures for handling and storing sensitive information (including Privacy Act, PII, or FOUO information). Employees who telecommute will follow any additional telecommuting computer security guidelines listed in Reclamation Form 7-2500-1 (8-98).

All users will be required to acknowledge a remote access banner that will appear during their login process. Variations in the presented banner may occur as a result of legal direction and users are encouraged to carefully review all banners before acknowledging. A remote access banner will appear, either in whole or abbreviated as necessary to meet space constraints, similar to the following:

***WARNING – Before you download Department of the Interior data to a computer or any other device capable of storing electronic data, you must comply with Department standards for data encryption and system security. You must also understand and agree to comply with Department requirements for deleting the data. Contact your IT Security Manager for specifications regarding these standards and requirements. Failure to comply may result in criminal, civil, and/or disciplinary action.***

Although the Department has formally accepted the risk of users accessing e-mail through the Microsoft OWA, users must ensure that all Department and Reclamation information downloaded to IT systems using remote access is erased from the systems after no more than 90 days or when the information is no longer needed.

Note: For further information see: *Department IT Security Policy: Access Control (AC)*

## **2.14 Backup**

Users are encouraged to store all important data on network shared drives. Backups containing, or which may contain, sensitive, restricted, or Privacy Act information must be stored in a secure manner.

Note: For further information see: *Department IT Security Policy: Contingency Plan (CP)*

## **2.15 Physical Protection and Security**

Users are responsible for the physical security of government IT equipment they have been assigned or are using. Portable equipment shall be protected from loss or theft at all times.

Government IT equipment shall not be checked with luggage when on travel, left in plain sight in rental or personnel vehicles, physically mistreated in any intentional manner, loaned to third parties without proper authorization, or left unattended in public places.

Users will obtain a property pass from the appropriate custodial officer before taking home any government owned IT equipment. Please be aware that a Reclamation property pass may also be required to take Reclamation IT equipment into other, non-Reclamation, government facilities.

Users must physically protect all hardware or software based authentication tokens entrusted to them for access control or encryption purposes. (A token is typically a physical device that an authorized user is given to demonstrate, for authentication purposes, that a user is authorized to access a specific IT resource.)

Note: For further information see: *Department IT Security Policy: Physical and Environmental (PE)*

## **2.16 Assignment and Limitation of System Privileges**

System privileges are limited to personnel who demonstrate both a need for system level access (for example, root access on Unix, administrator access on Windows, DBA access on database systems) and demonstrate an understanding of the responsibility that goes along with it.

All individuals with system level access agree to document any changes made while utilizing system level privileges and to inform the designated system administrator of these changes.

Users will not attempt to gain system level access through any unauthorized means.

For individual workstations assignment privileges will be granted appropriate to the user's duties. Where additional permissions are required, the user should sign an elevated privilege ROB and their account request form should be updated to identify the additional privileges.

## 2.17 System Monitoring

Users acknowledge that their use of government IT equipment and systems may be monitored for inappropriate use, and that there is no reasonable expectation of privacy in that use. Furthermore, any use of a government IT system constitutes consent to such monitoring. As users go through the steps to gain access to Reclamation IT resources, they will be required to acknowledge a banner that appears during their login process. Variations in the presented banner may occur as a result of legal direction and users are encouraged to carefully review all banners before acknowledging. The banner will appear, either in whole or abbreviated as necessary to meet space constraints, similar to the following:

***WARNING – This is a United States Government computer system, maintained by the Department of the Interior, to provide official unclassified U.S. Government information only. Use of this system constitutes consent to monitoring, retrieval, and disclosure by authorized personnel. Users have no reasonable expectation of privacy in the use of this system. Unauthorized use may subject violators to criminal, civil, and/or disciplinary action.***

Users also acknowledge that government IT equipment and systems may be monitored and/or tested for security. Identified vulnerabilities or areas of non-compliance will be immediately corrected or “patched” by an authorized system administrator.

## 2.18 Definitions<sup>§§</sup>

**Broadcast Transmission** is a message or e-mail note sent at once from a single user to many users and/or sites.

**Commercial gain activity** is defined as any activity involving or relating to buying, selling, advertising, leasing, or exchanging products or services for anyone's personal profit or gain. It includes day trading and buying or selling real estate for commercial purposes.

**Limited personal use** means activity that is conducted for purposes other than accomplishing official or otherwise authorized activities, and that does not adversely affect the employee's job performance and is further defined for each kind of equipment in section 2a thru section 2e.

<sup>§§</sup> Definitions from Departmental Manual: Section 410, Chapter 2, Paragraph 2.3

Title: <b>Bureau of Reclamation – General Rules of Behavior for Use of IT Systems and Equipment</b>	Date: <b>3/18/11</b>
--	-------------------------

**Non-duty time** is time when the employee is not expected to be performing official business. To the extent permitted by this policy, employees may, for example, use government office equipment during their own off-duty hours such as before or after a workday (subject to local office hours), lunch periods, authorized breaks, weekends or holidays (if their duty station is normally available to them at such times).

**Personally Identifiable Information** means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual."

Title:

**Bureau of Reclamation – General Rules of Behavior for Use of IT Systems and Equipment**

Date:

**3/18/11**

### **3. Acknowledgement**

By signing below, I acknowledge that I have read and understand Reclamation's Rules of Behavior (ROB) for the proper use and protection of IT systems and equipment. I understand that if I do not fully understand the expectations identified in this ROB, that I can contact my local IT management official or union representative. Furthermore, I understand that any misuse of the Reclamation IT systems and equipment assigned or entrusted to me could result in loss of IT systems use privileges and/or adverse disciplinary actions consistent with Department and Reclamation personnel policies.

---

*User's Name (please print)*

---

*User's Signature*

*Date*

***Please retain a copy of these Rules of Behavior for your records and return your signed copy to the RESC/Regional Service desk or to the individual designated as your Region or Office record keeper.***