

Appendix H: End User Rules of Behavior

1. Introduction

The Office of Management and Budget (OMB) has established the requirement for formally documented Rules of Behavior as set forth in OMB Circular A-130. The Rules of Behavior contained in this document are to be followed by users of Office of the Chief Information Officer (OCIO) information systems. Users will be held accountable for their actions on all OCIO information systems. If an employee violates DOE and/or OCIO policy the employee may be subject to disciplinary action at the discretion of DOE, OCIO, and/or their employer's management. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation and the judgment of the appropriate authority. These rules of behavior pertain to both classified (National Security Systems) and unclassified environments.

2. Appropriate Use of OCIO Resources

Use of Government Equipment and Resources

- Employees should not install software, copy software, or download software unless formally authorized by system owner
- Any individual who has information regarding suspected or actual violations of laws, regulations or policies should notify their supervisor, an Information System Security Officer (ISSO), the Office of the Chief Information Officer (OCIO), or the DOE Inspector General
- Employees should not download or install any peer-to-peer software, gaming software, or any other software that has not been authorized by the system's Designated Approving Authority (DAA)
- Employees are not authorized to disable any security features or alter system configurations
- Except as explicitly allowed according to the Limited Personal Use section below, the following are considered inappropriate use of Government equipment and resources:
 - Conducting private and or personal business activities
 - Using resources for amusement/entertainment purposes or to organize non-DOE sanctioned social events (including sending holiday cards)
 - Broadcasting non-business related email (sending email to a large distribution list) including sending or forwarding email chains
 - Viewing or transmitting any sexually explicit materials or any materials related to illegal activities
 - Using Government equipment and resources as staging grounds to gain unauthorized access to other systems

Internet

- There is a zero tolerance policy for inappropriate use of the Internet. Except as explicitly allowed according to the Limited Personal Use section below, the use of

Government equipment and official duty time for inappropriate non-work related use of the Internet is a violation of and standards of conduct

- Employees shall not knowingly introduce a computer virus into OCIO computers or networks or load removable media (e.g., diskettes, CDs, USB media, etc.) of unknown origin

Email

- Electronic messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of OCIO
- The Standards of Ethical Conduct for Employees for the Executive Branch provides that an employee “shall not use [Government] property or allow its use for other than authorized purposes.” The only approved exceptions are detailed in the following section “Limited Personal Use.”
- Users are responsible for the content of all text, audio, or images that (s)he places on the Internet or sends via email. All communications should have the employee’s name attached.
- User should not transmit copyrighted materials without written permission from the owner
- Employees are advised that OCIO electronic email communications are not encrypted by default. Email should not be used for sensitive data transmissions unless encryption or similar technologies are employed.

Limited Personal Use

- Federal Employees, contractors and other Government representatives are permitted limited use of government equipment or resources for personal needs when such use involves minimal additional expense to the government, is performed on the employee’s non-work time, does not interfere with the mission or operations of DOE HQ activities and does not violate the Standards of Ethical Conduct for Employees of the Executive Branch. Examples of acceptable use are:
 - Communication with a volunteer charity organization
 - Checking a Thrift Savings plan or other investments
 - Sending an occasional fax to transmit a form for personal reasons (e.g. loan or other application)

3. Incident Handling and Reporting

Upon the discovery of a security-related incident, the employee should immediately stop work, report cyber security incidents (suspected or actual) to management and contact the help desk immediately upon discovery. Reportable cyber security incidents generally meet at least one of the following criteria:

- All attempts at unauthorized access, whether or not they are successful, even if unauthorized access is suspected but not yet proven
- Instances of malicious code such as viruses, Trojan horses, or worms
- Situations where a person who does not appear to be conducting legitimate business is acting in a manner that raises suspicion
- Instances where a user is in violation of these Rules of Behavior, or exhibiting non-compliance with DOE or OCIO policy

- Actual or probable loss of media containing PII, or the disclosure of PII to unapproved individuals

4. Media Contamination and Sanitization

- Should an end user discover or be notified of the possibility that their workstation, PDA, or network files may have been contaminated due to inadvertent receipt of classified information, they should immediately cease operation and contact their manager and the ISSO. The ISSO will arrange for the clearing or sanitization of the devices or files as appropriate. The ISSO will notify the user when it is acceptable to resume operation
- If the workstation, PDA, or other device has been involved in an incident (defined above in section 3 “Incident Handling and Reporting”) or contaminated with classified information the ISSO must be notified prior to commencing media sanitization procedures

5. Access Controls

Password Generation (pertains to unclassified systems only)

- Passwords should contain at least eight non-blank characters consisting of a combination of letters (preferably a mixture of upper and lowercase), numbers, and at least one special character within the first seven positions
- Passwords should contain non-numeric characters in the first and last position
- Passwords should not contain the user ID, any common English dictionary word, spelled forward or backwards (except words of three or fewer characters); employ common names; or include the user’s own or, to the best of his/her knowledge close friends—or relatives—names, employee serial number, Social Security number, birth date, phone number, or any recognizable information associated with the user of the password. Passwords should not contain any simple pattern of letters or numbers, such as “qwertyxx” or “xyz123xx.”

Password Management

- Passwords employed by the user on unclassified systems should be different than the passwords employed on classified systems
- Individuals should change passwords:
 - At least every 6 months
 - Immediately after sharing
 - As soon as possible, but within 1 business day after a password has been compromised, or after one suspects that a password has been compromised
 - On direction from management
- Individuals should not:
 - Share passwords except in emergency circumstances or when there is an overriding operational necessity
 - Leave clear-text passwords in a location accessible to others or secured in a location whose protection is less than that required for protecting the information that can be accessed using the password
 - Enable applications to retain passwords for subsequent reuse

6. Remote Access

- Remote access users must be authorized for remote access by the system owner and should access only the services for which they have been explicitly authorized
- All remote access must be via VPN and utilize OCIO's two-factor RSA token authentication solution
- Remote access to OCIO internal systems that circumvents intended remote access controls is expressly prohibited (e.g. accessing an internal system directly using a modem on the internal system)
- Anti-virus software must be used on all remote machines and must be updated with the latest virus definitions prior to initiating a remote session

7. Protection of Sensitive Unclassified Information

- Each employee (both Federal and contractor) using OCIO information systems is responsible for identifying sensitive unclassified information (SUI), which includes personally identifiable information (PII), on their individual portable devices (i.e. laptops, PDAs) or removable media (i.e. thumb/flash drives, CDs)
- If there is a critical business need to store SUI on portable devices or removable media and transport it outside a secure DOE facility or access SUI remotely (i.e. VPN), the employee must submit detailed justification to and obtain approval from the information system's DAA unless otherwise specified in the relevant system's SSP.
- If there is a critical business need to store PII on portable devices or removable media and transport it outside a secure DOE facility or access Protected PII remotely (i.e. VPN), the employee must submit detailed justification to and obtain approval from the information an official delegated the authority by the ACIO.
- If the employee obtains approval for the storage or access requirements above, the following actions must be taken:
 - All SUI must be safeguarded in compliance with the *Sensitive Unclassified Information and Privacy* section of the OCIO PCSP.
 - SUI transported outside the secure facility must be encrypted using a FIPS 140-2 compliant method and must be removed from the device within 90 days using a DOE approved method which renders the data unrecoverable (merely deleting the SUI is insufficient).
 - Remote access to SUI requires two factor authentication (password only is insufficient) and the remote session must timeout after 30 minutes of inactivity requiring re-authentication.
- If SUI is transmitted via electronic means (i.e. E-Mail, FTP), the information must be encrypted using a FIPS 140-2 compliant method
- SUI is not permitted to be stored or processed on personally owned computer equipment
- If a device containing protected PII is lost or stolen, or there is reason to suspect that unauthorized individuals have gained access to protected PII, it must be reported within 45 minutes of discovery

8. Personally Owned Devices

- Employees (both Federal and contractors) are prohibited from connecting Personally Owned Devices (PODs) to OCIO information systems. PODs are information systems, devices, media, or equipment owned by individuals and entities. PODs include, but are not limited to, personal computers and related equipment, handheld PDA devices, facsimile machines, photocopiers, enhanced cell phones, and storage devices such as flash memory (memory sticks), flash cards, portable hard drives, and MP3 players.
- If there is a critical business need to connect PODs to OCIO resources, the employee must submit detailed justification to and obtain approval from the information system's DAA.

I acknowledge receipt of, understand my responsibilities, and will comply with these rules of behavior for OCIO Information Systems.

Printed Name of User

Signature of User

Date