UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

MIGRATION PLANNING GUIDANCE TEMPLATES

COMMON RULES OF BEHAVIOR POLICY

May 23, 2008

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Working for America

Table Of Contents

1. Purpose, Scope and Objectives 1
2. General Rules of Behavior for HR LOB SSC Customers 2
3. Additional Rules for Security and Administration Users 5
4. Remote Access Off-Site 5

1. Purpose, Scope and Objectives

The Rules of Behavior dictate the minimum responsibilities and expectations of all individuals with access to Shared Service Centers' (SSC) Information Technology (IT) systems. All individuals will review and provide a signature (hardcopy or digital) or electronic verification agreeing to uphold these rules prior to receiving SSC Agency and/or Customer Agencies Local Area Network (LAN) access. These Rules of Behavior will be reinforced within the context of annual Information Assurance training. The SSC customer will provide a training course that will describe, at a minimum, the acceptable use requirements for the SSC systems contained within this policy.

What is the purpose of the Rules of Behavior?

Rules of Behavior summarize laws and guidelines from various SSC Agency and other Federal documents, most specifically OMB Circular A-130 and Section 208 of the E-Government Act of 2002. In addition, Rules of Behavior establish a minimum set of rules of behavior to which each Share Service Center (SSC) Customer user is expected to adhere to when accessing their respective SSC system. SSC Customer Agencies will use these guidelines as a basis for their own security plans.

What are Rules of Behavior?

Rules of Behavior function as part of a comprehensive program to provide complete information security. These guidelines are created to hold users accountable for their actions and responsible for information security. Rules of Behavior establish standards of behavior in recognition that knowledgeable users are the foundation of a successful security program. Users need to understand that taking personal responsibility for the security of their computer and the data it contains is an essential part of their mission.

Who is covered by these rules?

The General Rules of Behavior apply to all SSC Customer users (civilian, military, and contractor) with access to the SSC systems. SSC Customer users should be fully aware of, and comply with their respective Agency policies, as well as the respective SSC Agency policies.

What is the importance of these rules?

User compliance is an essential component of the overall SSC's Agency security policy. It applies to the use of computer generated data, as well as to the use of procedures and policies related to software installation, password protection, and adherence to standard e-mail policies. All SSC Customer users must comply with the policies put forth in this Rules of Behavior policy. Because written guidance cannot cover every contingency, SSCs and SSC Customer staff and users are asked to augment these rules and use their best judgment and

highest ethical standards to guide their actions. Because these principles are based on federal laws and regulations, and SSC unique specific regulations and directives, there are consequences for failure to comply with the principles of behavior. Depending on the severity of the violation, sanctions may include a verbal or written reprimand, the removal of IT system access for a specified time, or a reassignment to other duties, demotion, or termination. Misuse of Privacy Act and/or sensitive, classified data may result in civil and criminal charges and/or fines.

In order to ensure that the security requirements of availability, integrity, confidentiality, and accountability are met, policies and procedures will be put in place to facilitate the proper operation and protection of their respective systems. These rules are intended to enhance existing SSC policy and further define the specific rules each SSC Customer user must follow while accessing an SSC system. Because written guidance cannot cover every contingency, SSCs and SSC Customer users are asked to augment these rules and use their best judgment and highest ethical standards to guide their actions.

2. General Rules of Behavior for HR LOB SSC Customers

Users will:

- Safeguard the information processed, stored, and transmitted on SSC and SSC Customer systems from unauthorized or inadvertent modification, disclosure, destruction and use. SSC IT systems are for official use only and authorized purposes in accordance with SSC specific ethics regulation.
- Comply with safeguards, policies, and procedures to prevent unauthorized access to SSC IT systems.
- Comply with the terms of software licenses and only use SSC-licensed and authorized software.
- Refrain from engaging in deliberate activities that overload network resources (e.g., downloading large music or video files). Network bandwidth consumption caused by such downloads may inhibit or prohibit network service to other users.
- Recognize the accountability assigned to each user. Each user must have a unique ID to access the SSC Customer LAN. Individual user activity will be recorded, including Internet and Intranet sites and files accessed.
- Minimize the risk of having the system compromised as a result of poor password selection.
- Assume responsibility for selecting passwords that are difficult to guess. Whenever technically supported, as many as possible of the following password selection criteria should be employed:
    1. Passwords must be case sensitive.
    2. Passwords must contain a mix of at least two (2) lowercase letters, two (2) uppercase letters, two (2) numbers, and two (2) special characters.
    3. Dictionary words, derivatives of User Ids, and common character sequences such as “123456” may not be used.

4. Proper names, geographical locations, common acronyms, and slang should not be used.

- Report all instances of actual or potential security incidents, or any incidents of suspected fraud, waste or misuse of SSC systems to appropriate officials.
- Log out prior to leaving his/her work area at the end of the day. User will lock the workstation or log off an active session when leaving the workstation for any reason (e.g., going to a meeting, lunch, restroom, etc.) to prevent unauthorized use of the user's logon session. A password-controlled screensaver is an acceptable means for satisfying this requirement, provided the screensaver is activated before leaving the workstation and the screensaver password complies with appropriate SSC password rules.
- Complete the SSC approved Information Security Awareness. Training should be completed prior to obtaining access to the SSC Agency system and on an annual basis thereafter.
- Be cognizant of the respective SSC IA and Customer-specific IA policies.
- Refrain from using his or her trusted position and access rights to exploit system control or access data for any reason other than in the performance of official duties.
- Include the following disclaimer on e-mail and/or fax cover sheet when transmitting sensitive data from the system:
- Encrypt sensitive information when reasonable and worthwhile.
- Comprehend that information systems containing personally identifiable information (e.g., SSN, name, photo, and patient ID number) must be covered by a Privacy Act System of Record (SOR) Notice, and will likely have added security controls that must be followed.

Each SSC establishes its own policies for determining which employees may work at home or in other remote workplace locations. To ensure the security of the SSC systems, all remote work management should include:

- Provisions for the authentication of the remote user through the use of ID, password, or any other acceptable technical means.
- Adequate storage of files, removal and on-recovery of temporary files created in processing sensitive data, virus protection, intrusion detection, and physical security for government equipment and sensitive data.
- A management/employee agreement that, at a minimum, outlines the work to be performed and the security safeguards and procedures the employee is expected to follow.

Users will not:

- Permit another person to use or share his/her log-on session. Because the log-on session is directly associated with an individual User ID, the user is personally accountable for all actions performed with the User ID.
- Modify automated screen-lock functions performed by the IT system.
- Download and/or open files from un-trusted sources.

- Use shared drives to relay Privacy Act data, unless the data is password protected and the folder within the shared drive has access set up only for those authorized to access the data.

Managers will:

- Plan for disaster recovery and contingency situations.
- Determine access levels based on the user's duties and need-to-know.
- Provide first line approval for employee access when stipulated by organizational policies.

Information Technology (IT) service providers:

IT service providers include (but are not limited to): system administrators, computer operators, system engineers, network administrators, LAN server administrators, those who have access to change control parameters for equipment and software, database administrators, those who control passwords and access levels, and troubleshooters/system maintenance personnel. IT service providers must:

- Restrict system access to those persons needed to perform assigned duties.
- Delete or reassign accounts as soon as customer users leave.
- Plan for disaster recovery and contingency situations.
- Post logon warning banners at all logon points to government computers and systems where technically practical.
- Set passwords for new accounts. Password setup will include the following:
  - Passwords will be changed every 90 days.
  - Password history will be set to a minimum of (5).
  - Unsuccessful logon attempt counter will be set to (3) with a counter reset of no less than 60 minutes. This allows no more that two (2) unsuccessful logon attempts within a 60-minute period.
  - After the third unsuccessful logon attempt, the account lockout duration will be set to "forever" requiring the account to be unlocked by a system administrator.
  - System messages will display a legal warning, which requires the user to consent to monitoring. This consent is currently on the warning banner on all government operated computer systems.
  - The "display the username of the last successful logon" feature will be disabled.
  - The last successful logon message feature that tells the user the last successful and unsuccessful logon time and date will be enabled.

3. Additional Rules for Security and Administration Users

Security and administration personnel will:

- Advise the system owner on matters concerning information technology security.
- Assist the system owner in developing security plans, risk assessments, and supporting documentation for the certification and accreditation process.
- Ensure that adequate physical and administrative safeguards are operational within their areas of responsibility and that access to information and data is restricted to authorized personnel on a need-to-know basis.
- Verify that users have received appropriate security training before allowing access to any SSC system.
- Document and investigate known or suspected security incidents or violations and report them to the SSC Information Security Officer and systems owner.

4. Remote Access Off-Site

Personnel will:

- Adhere to all SSC and Customer Agency provisions or agreements related to off-site work.
- Use virus protection software on all off-site systems used to access SSC systems and keep the virus protection software up-to-date.
- Change remote access passwords frequently.
- Protect remote access passwords from access by other individuals and do not store passwords in login scripts, batch files or elsewhere on the computer.

UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
1900 E Street, NW
Washington, DC 20415

HRLOB/CRBP052008