Attachment II

Office of Residential Care Facilities

232 Healthcare Portal

Rules of Behavior

Background

What are Rules of Behavior?

Office of Management and Budget (OMB) Circular A-130 Appendix III requires every System Security Plan (SSP) to contain a Rules of Behavior (ROB). Rules of Behavior are part of a comprehensive program to provide complete information security. These guidelines were established to hold users accountable for their actions and responsible for information security. Rules of Behavior establish standards of behavior in recognition of the fact 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 job.

Who is covered by these Rules?

These rules extend to all HUD personnel and any other persons using HUD IT equipment or accessing HUD systems under formally established agreements. This includes contractors and other federally funded users.

What is Sensitive Data?

Sensitive data is data that must be protected on the basis of its need for protection against loss, disclosure, or alteration because of the risk and magnitude of harm that could result.

What are the penalties for Non-compliance?

Users who do not comply with the prescribed Rules of Behavior, are subject to penalties that can be imposed under existing policy and regulations, including official, written reprimands, suspension of system privileges, temporary suspension from duty, removal from current position, termination of employment, and even criminal prosecution. HUD will enforce the use of penalties against any user who willfully violates any HUD or federal system security (and related) policy as appropriate.

User Rules of Behavior

This section identifies the Rules of Behavior that apply to the ORCF Healthcare Portal end-users.

Passwords

1. Passwords should be a minimum of eight characters, and be a combination of letters, numbers and special characters (such as *#$ %). Dictionary words should not be used.
2. Passwords will be changed at least every 90 days and should never be repeated. Compromised passwords will be changed immediately.

3. Passwords must be unique to each user and must never be shared by that user with other users. For example, colleagues sharing office space must never share each other's password to gain system access.
4. Users who require multiple passwords should never be allowed to use the same password for multiple applications.
5. Passwords must never be stored in an unsecured location. Preferably, passwords should be memorized. If this is not possible, passwords should be kept in an approved storage device, such as a Government Services Administration Security Container. If they are stored on a computer, this computer should not be connected to a network or the Internet. The file should be encrypted.

Safeguarding Information

To properly safeguard the Department's information assets while using information technology, it is essential for all employees to be aware of procedures for destroying sensitive information. Sensitive information within HUD that must be protected includes, but is not limited to, financial management information (budgeting, accounting, etc.); investigative information; contract sensitive information (pre-solicitation procurement documents, statements of work, etc.); and security management information (i.e., identification of systems security controls and vulnerabilities).

Of particular concern is Personally Identifiable Information (PII), which includes social security numbers, names, dates of birth, places of birth, parents' names, credit card numbers, applications for entitlements, and information relating to a person's private financial, income, employment, tax records, etc.

To assist you in determining what type of information should be considered sensitive, here are a few examples:

1. Personnel data
2. Procurement documents
3. Statements of Work or related procurement documents
4. Loan applications or files
5. COOP data

Security Practices

1. Using system resources to copy, distribute, utilize, or install unauthorized copyrighted material is prohibited.
2. Users who no longer require system access (as a result of job change, job transfer, or reassignment of job responsibilities) must notify the system administrator.
3. When not in use, workstations must be physically secured. Users must also log-off or turn-off the system.
4. Movable media (such as diskettes, CD-ROMs, and Zip disks) that contain sensitive and/or official information must be secured when not in use.
5. Altering code, introducing malicious content, denying service, port mapping, engaging a network sniffer, or tampering with another person's account is prohibited.
6. If a user is locked out of the system, the user should not attempt to log-on as someone else. Rather, the user should contact the system administrator.
7. HUD users are responsible for attending annual IT Security training. Failure to attend will result in having system access privileges revoked.

System Administrator Rules of Behavior

System administrators have a unique responsibility above and beyond that of regular users. In addition to being regular system users, they also have special access privileges that regular users do not have. Therefore, they need to be susceptible to additional Rules of Behavior over and above the common user.

1. System administrators may only access or view user accounts with the expressed consent of the user and/or management.
2. System administrators may not track or audit user accounts without the expressed consent of the user and/or management.
3. System administrators must make every reasonable effort to keep the network free from viruses, worms, Trojans, and unauthorized penetrations.
4. It is the system administrators' responsibility to account for all system hardware and software loaned to system users for the execution of their official duties.
5. HUD system administrators are responsible for attending annual IT Security training. Failure to attend will result in having system access privileges revoked.

Additional rules of the system follow:

1. Log off the system when leaving the system/workstation area.
2. Refrain from leaving written passwords in the workstation area.
3. Passwords for application system must be changed periodically, and the rules for length, composition (uppercase/lowercase, numeric) and reuse are dependent on individual application controls.
4. Your User ID will be suspended after 45 days of inactivity and you will need to contact the help desk for a Password reset.
5. Your User ID will be terminated after six months of inactivity, and you will need to re-apply for access to the system.
6. Avoid posting printouts of sensitive output data on bulletin boards.
7. Avoid leaving system output reports unattended or unsecured.
8. Control input documents by returning them to files or forwarding them to the appropriate contact person in your office.
9. Avoid violation of the Privacy Act, which requires confidentiality of personal data contained in government and contractor data files.
10. Report immediately any security violations to the help desk.
11. Respond to any requests for information from HUD officials regarding system security practices.