Rules of Behavior For
Access and use of
Commission Corps (CC)
SYSTEMS

1. Introduction

The following rules of behavior are to be followed by all users (contractors and employees) that use any networked or standalone Systems that supports the mission and functions of the Commission. The rules in Section 3 clearly delineate responsibilities and expectations for all individuals with access to these systems.

Non-compliance of these rules will be enforced through sanctions commensurate with the level of infraction. Actions may range from a verbal or written warning and/or removal of system access for a specific period of time depending on the severity of the violation.

2. Other Policies and Procedures

Rules of Behavior (RoB) provide general instructions on the appropriate use of Departmental IT resources and apply to all Departmental users, including both civil servants and contractors. All government and contractor staff is required to read this document and sign and submit the appropriate form(s) before accessing Departmental systems and or networks.

The *HHS Rules of Behavior* are not to be used in place of existing policy. Rather, they are intended to supplement the *HHS Information Security Program Policy* and the *HHS Information Security Program Handbook*. Because written guidance cannot cover every contingency, Departmental 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 Departmental regulations and directives, there are consequences for failure to comply with the principles of behavior. Violation of these rules may result in suspension of access privileges, written reprimand, suspension from work, demotion, and criminal and civil penalties.

All government and contractor staff must sign the appropriate form, acknowledging that they have been made aware of and understand the requirements and responsibilities outlined in this document and the *Secure One HHS* policies which can be found at http://intranet.hhs.gov/infosec/policies_guides.html. Questions about these ROB may be directed to one's supervisor or Contracting Officer's Technical Representative (COTR), or to the Operating Division (OPDIV) Chief Information Security Officer (CISO).

Activities on Departmental network system resources are subject to monitoring, recording, and periodic audits. Authorized IT security personnel may access any "user's" computer system or data communications and disclose information obtained through such auditing to appropriate third parties (e.g., law enforcement personnel). Use of Departmental IT system resources expresses consent by the user to such monitoring, recording, and auditing.

3. CC Systems Rules

3.1 To ensure individual accountability of actions performed in any CC System, users are responsible for understanding and complying with all password use requirements. Passwords are an important aspect of computer security and are the front line of protection for user's accounts. Users are to abide by the password requirements as outlined in the *Secure One HHS* policies which can be found at *http://intranet.hhs.gov/infosec/policies_guides.html*, including the need for adequate (difficult to decipher) passwords that are a minimum of 8 characters in length and contain at least one number, one capital letter, and one lowercase letter to insure the password is difficult to decipher, the necessity for changing passwords at least every 90 days, and the requirement to not share or disclose passwords.

3.2 Users are not allowed to exceed their authorized access limits in any CC System by changing information or searching databases beyond the responsibilities of their job or by divulging information to anyone not authorized to know that information.

3.3 No inter-connections to other CC Systems or transfer of CC Data to other information systems is authorized beyond those established as part of the standard authorized processing requirements of any CC System.

3.4 No user having access to any CC System will disable any encryption established for network, internet and web browser communications.

3.5 No direct dial-in access to any CC System has been established nor is authorized.

3.6 All personnel, as well as contractors, that are responsible for developing and maintaining any CC System, must comply with all copyright license regulations associated with CC software. Managers must ensure that government personnel and Contractor personnel understand and comply with license requirements. End users, supervisors, and functional managers are ultimately responsible for this compliance

3.7 Users should be aware that personal use of information resources is authorized on a limited basis within the provisions of "HHS IRM Policy for Personal Use of Information Technology Resources"

3.8 Users are required to report all instances of actual or potential security violations to their supervisors, Information Technology Security Officer, and Information Systems Security Officer.

3.9 Each subscriber organization establishes its own policies for determining which employees may work at home or in other remote workplace locations. Any remote work arrangement, to insure the security of CC systems, should include:

- Provisions for the authentication of the remote user through the use of ID and password or other acceptable technical means.
- 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.
- Ensure adequate storage of files, removal and non-recovery of temporary files created in processing sensitive data, virus protection, intrusion detection, and physical security for government equipment and sensitive data.
- Established mechanisms to back up data created and/or stored at alternate work locations.

3.10 In receiving access to an CC System, the user agrees to the following Security & Confidentiality agreement:

(1) Maintain confidentiality and follow all applicable IT system security policies and procedures issued by the Department as outlined in the *Secure One HHS* policies which can be found at *(http://intranet.hhs.gov/infosec/policies_guidelines.html*

(2) Comply with the following listed regulations and any other applicable Public Policy and Law as listed in the:

A. Code of Ethics for Government Service (P.L. 96-303) as pertains to IT Resources

B. Privacy Act of 1974, 12/31/74, (P.L. 93-579).

C. Counterfeit Access Device & Computer Fraud & Abuse Act of 1984, 10/12/84.

D. Computer Security Act of 1987, January 8, 1988, P.L. 100-235.

E. Computer Crime Act of 1984.

F. Disclosure of Confidential Information Generally, 18 U.S.C. 1905 (1948).

G. Freedom of Information Act, 5 U.S.C. 552 (1967)

H. OMB Circular A-130 “Appendix III”

(3) Comply with the following listed DHHS rules and any other applicable rules as listed in the Automated Information Systems Security Handbook, Appendix A Section H (materials available from site security rep.):

A. DHHS General Administration Manual Chapter 7, Physical Security Policy, and part 45, Privacy Act Guidance

B. DHHS Information Resources Management Manual, Part 6, AIS Security Training and Orientation Program Guide.

C. DHHS Internal Controls Manual,

D. Chapter 5-45 Code of Federal Regulations (CFR), DHHS Freedom of Information Act Regulations

E. 45 Code of Federal Regulations (CFR), Subpart 5B, DHHS Privacy Act Regulations

(4) Notify application administrator, security administrator, or CC system owner when access is no longer required.

In concurrence, the employee’s supervisor agrees

(1): Make all applicable IT systems security policies and procedures and all the pertinent parts of the above listed items issued by the Department available to the requestor and monitor compliance with them.

(2) Notify application administrator, security administrator, or CC system owner when access is no longer required.

4. Additional Rules for Security and Administration Users

Security and system administration personnel have significant access to processes and data in any CC System. As such, the System Security Administrators, Systems Administrators, and Database Administrators have added responsibilities to ensure the secure operation of any CC System

Security and administration personnel are to:

- o Advise the system owner on matters concerning information technology security.
- o Assist the system owner in developing security plans, risk assessments, and supporting documentation for the certification and accreditation process.
- o Ensure that any changes to any CC System that affect contingency and disaster recovery plans are conveyed to the person responsible for maintaining continuity of operations plans for CC Systems.
- o 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.
- o Verify that users have received appropriate security training before allowing access to any CC System.
- o Implement applicable security access procedures and mechanisms, incorporate appropriate levels of system auditing, and review audit logs.
- o Document and investigate known or suspected security incidents or violations and report them to the ISSO, ITSO, and systems owner.