Department of Justice (DOJ)
Computer System User Information Technology (IT) Security
General Rules of Behavior
May 21, 2004

Introduction

Purpose

The intent of the Computer System User IT Security General ROB is to summarize laws and guidelines from various federal and DOJ documents, most specifically OMB Circular A-130, DOJ Order 2640.2 (series), and the DOJ IT Security Standards, for the use of DOJ computing resources. They are to be followed by all users (contractors and DOJ employees) who use any computing resources that support the mission and functions of the Department of Justice. In order to remain in compliance with all applicable laws, regulations, and DOJ Standards, the DOJ reserves the right to update these Rules of Behavior at any time.

What are "Rules of Behavior (ROB)"?

The ROB are part of a comprehensive program to provide complete information security. ROB establish standards of actions in recognition of the fact that knowledgeable users are the foundation of a successful security program. The ROB concern use of, security in, and the acceptable level of risk for, DOJ systems, and highlight the need for users to understand that taking personal responsibility for the security of a computer and the data it contains is an essential part of their job. People are the first line of defense in support of DOJ/Office/Bureau/Component information and information systems. Users offer many eyes and ears to detect and report threats to DOJ information systems.

Who is covered by these rules?

These rules extend to all DOJ personnel (civilians and contractors) and any other persons using DOJ computing resources or accessing DOJ systems under formally established agreements. All users should be fully aware of, and abide by, DOJ security policies as well as related federal policy contained in Privacy Act, Freedom of Information Act, and DOJ Records Management Regulations. All users will review and provide signature or electronic verification to these rules annually.

What are the penalties for Noncompliance?

Compliance with these rules will be enforced through sanctions commensurate with the level of infraction. Actions may include 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. In addition, activities that lead to or cause the disclosure of classified information may result in criminal prosecution under the U.S. Code, Title 18, Section 798, and other applicable statutes.

Responsibilities

Complying Users will:

1. Process, store, and/or transmit classified data only on systems and/or networks authorized for the highest level of the classified data involved.
2. Protect and safeguard DOJ information including media that contains information from unauthorized access, unauthorized or inadvertent modification, disclosure, destruction, denial of service, or use in accordance with applicable Department policy, practices, and procedures (DOJ Order 2640.2 (series), DOJ IT Security Standards).
3. Protect all hard copy produced at the highest classification or sensitivity level of that system until reviewed for proper classification or sensitivity and control.
4. Destroy information or media, when required, in accordance with security requirements based on the level of classification or sensitivity.
5. Provide access to classified or sensitive information only after ensuring that the parties have the proper clearance, authorization and need-to-know.
6. Operate the computer only in those areas approved for the highest classification or sensitivity level of the information involved unless specific authorization has been received from the Information System Security Officer to operate the computer in other areas.
7. Store the computer in an approved security container (or in a facility approved for open storage) when it is not in use.
8. Never remove the computer (or hard drive) from authorized or cleared DOJ facilities without specific approval of the Information System Security Officer (ISSO).
9. Comply with terms of software licenses and only use DOJ-licensed and authorized software.
10. Use DOJ systems for lawful, official use, and authorized purposes in accordance with current guidelines (DOJ Order 2640.2 (series), DOJ IT Security Standards).
11. Use the e-mail system in accordance with DOJ guidelines (DOJ Order 2640.2 (series), DOJ IT Security Standards).
12. Not generate or send offensive or inappropriate e-mail messages, images, or sound files. Limit distribution of e-mail to only those who need to receive it. NOTE: Users are typically identified as a DOJ computer user when logged onto the Internet.
13. Choose and change passwords in accordance with DOJ IT Security Standard 3.1.
14. Not share account passwords with anyone.
15. Protect passwords at the highest classification and data sensitivity level of information on that system.
16. Know the system data and properly classify and protect all data inputs and outputs according to their sensitivity and value.

17. Properly mark and label sensitive and classified documents and media in accordance with the DOJ Security Program Operating Manual.
18. Ensure that sensitive information is removed from hard disks that are sent out for maintenance. For classified data, consult with the appropriate ISSO and the DOJ Security Program Operating Manual for sanitization procedures for hard drives.
19. Screen-lock the computer or log off when leaving the work area, and power down the computer when departing for the day.
20. Use authorized virus-scanning software on the workstation or PC. Know the source before using diskettes or downloading files.
21. Not use shared drives to store, maintain, or relay Privacy Act data unless the data is password protected and the folder within the shared drive has access set up only for those employees authorized to work with the data.
22. Complete an annual IT security awareness refresher course (the DOJ Computer Security Awareness Tool (CSAT) or equivalent).
23. Sign all logs, forms, and receipts as required for accomplishment of duties relating to the collection, use, transfer, or disposal of DOJ information or information systems.
24. Know who their ISSO is for each computer system. Consult the appropriate ISSO and obtain permission or approval before doing any of the following:
    - Changing any configurations and/or settings of the operating system and security-related software on classified systems.
    - Installing any software.
    - Adding, modifying, or removing hardware accessories or networks to a classified computer.
    - Accessing the internal components of the computer.
    - Testing the capabilities of the security control software.
    - Circumventing the security mechanisms used on and by the computer.
    - Attempting to access any electronic audit trails that may exist on the computer unless specifically authorized to do so.
25. Make the computer available at any time to the ISSO for inspection and review of audit logs.
26. Make the computer available at any time to the System Administrator for the installation of patches and other system administration activities.
27. Report known or suspected incidents immediately. Immediately report to the ISSO any evidence of tampering with the computer or if the computer's tamper-evident seals are broken.
28. Notify the ISSO when access to the computer is no longer needed (e.g., transfer, termination, leave of absence, or for any period of extended non-use).

29. Never perform audit functions on a system for which the user is either a user or system administrator.

In addition to the above Department of Justice General Rules of Behavior,

System Administrators will:

1. Ensure that the Certification Agent (CA) or a CA-appointed agent validates system security at least annually.
2. Make the computer(s) available for periodic reviews of the security configuration by independent testers.
3. Ensure that under no circumstances the same person serves as the system administrator and ISSO for the same system.

Managers will:

4. Ensure that staff has access to, and sufficient time to complete, the DOJ Computer Security Awareness Training (CSAT), or other annual IT security training offered by offices/bureaus/components not utilizing CSAT.
5. Ensure that staff has access to, and are aware of, all existing DOJ policies and procedures (DOJ Order 2640.2(series), DOJ IT Security Standards) relevant to the use of DOJ information technology resources.
6. Ensure that staff follows system security policies, guidelines and procedures (DOJ Order 2640.2(series), DOJ IT Security Standards).

I acknowledge receipt of the General Rules of Behavior listing, understand my responsibilities, and will comply with the rules of behavior for DOJ systems.

_____ _____

Signature Date