Department of Justice (DOJ)
Information Technology (IT) Security
Rules of Behavior for Privileged Users
May 21, 2004

Introduction

Purpose

The intent of the DOJ Rules of Behavior (ROB) for Privileged Users is to recognize the additional responsibilities associated with special access to, and/or privileges associated with, computer resources within the Department or its offices/bureaus/components. The ROB for Privileged Users are in addition to the Computer System User IT Security General ROB to which all DOJ users are subject. The identification of these responsibilities originates in OMB A-130 and is included in the DOJ IT Security Standards. These ROB for Privileged Users should be used as the basis for establishing Privileged User ROB for all such users within DOJ. 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.

"Privileged User" defined:

A privileged user is someone authorized access to departmental/office/bureau/component computer resources when that access provides the capability to alter the properties, behavior or control of the information system/network. It includes, but is not limited to, any of the following types of access:

a. "Super user," "root," or equivalent access, such as access to the control functions of the information system/network, administration of user accounts, etc.
b. Access to change control parameters (e.g., routing tables, path priorities, addresses) of routers, multiplexers, and other key information system/network equipment or software.
c. Ability and authority to control and change program files, and other users' access to data.
d. Direct access to operating system level functions (also called unmediated access) that would permit system controls to be bypassed or changed.
e. Access and authority for installing, configuring, monitoring or troubleshooting the security monitoring functions of information systems/networks (e.g., network/system analyzers; intrusion detection software; firewalls) or in performance of cyber/network operations.

Who is covered by these rules?

These rules extend to all privileged users (contractors and DOJ employees) who use any computing resources that support the mission and functions of the Department of Justice. All privileged users will review and provide signature or electronic verification to these rules annually, or upon change of assigned responsibilities, whichever occurs first.

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 Privileged Users will:

1. Understand that it is their responsibility to comply with all security measures necessary to prevent the unauthorized disclosure, modification, or destruction of information; follow appropriate system security policies, guidelines and procedures (DOJ Order 2640.2(series), DOJ IT Security Standards).
2. Grant read or write authority no higher than is granted to him/her (e.g., a component level user administrator shall not assign department level access to another user administrator).
3. Access application programs only for the purpose of creating or maintaining files.
4. Not make modifications to system configurations that could impact availability or security of the system without the approval of the Change Control Board and/or change management process.
5. Not perform general user activities under the same account (user name and password) due to the security requirement for separation of duties.
6. Protect all passwords from unauthorized disclosure.
7. Not share accounts with another privileged user.
8. Make the system available at any time to the ISSO for inspection and review of audit logs.
9. Make the computer(s) available for periodic reviews of the security configuration by independent testers.
10. Make changes to system configuration as directed to meet Vulnerability and Patch Management requirements.
11. Ensure compliance with software and copyright laws.
12. Immediately record and report any security incidents to the ISSO.
13. Notify the ISSO when access to a system is no longer required

---

I acknowledge and understand the responsibilities associated with my role as a Privileged User, and I will comply with the Privileged User Rules of Behavior.

_____ _____

Signature Date