



## DO Information Systems Rules of Behavior

### I. Overview

Rules of Behavior (ROB) describe security controls associated with user responsibilities and certain expectations of behavior for following security policies, standards, and procedures. As required by Office of Management Budget (OMB) Circular A-130, Department of the Treasury Directive 85-01, Departmental Offices (DO) Policy Handbook P-910, and, as specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, agencies are required to implement rules which delineate the responsibilities and expected behavior of all individuals with access to information systems. This document specifies the ROB for all DO employees who have access to DO information systems. All DO employees must agree to this ROB document prior to gaining access to any DO information system. If the ROB is updated or modified, DO will post the new version so that all users will be able to view the new ROB document.

### II. Background

Treasury Directive 85-01, DO Policy Handbook P-910, the Federal Information Systems Management Act of 2002 (FISMA), and the Computer Security Act of 1987, require all individuals involved with the management, use, or operation of a Federal computer system within or under the supervision of a Federal agency to be informed of their responsibilities for the use and protection of the system, the release of information, and the consequences of behavior not consistent with the rules. OMB A-130 requires that each information system user acknowledge acceptance of the Agency's acceptable ROB for the system before being allowed access to system resources. ROB establishes standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users must understand that taking personal responsibility for the security of all DO information stored, processed, and transmitted is an essential part of their job.

### III. General Terms and Conditions

All users must be alert at all times to possible breaches in security and adhere to the security regulations that have been established by the Department of the Treasury and the DO. OMB Circular A-130, Department of the Treasury Directive 85-01, and DO Policy Handbook P-910 require all Treasury information system users to receive annual security awareness and training as well as periodic refresher training.

These general terms and conditions serve to clarify the roles of management and system administration, and serve to provide notice of what is considered expected use of all DO information systems and behavior of DO users:

- I understand that I have **NO** expectation of privacy in accessing or using any DO or other Federal government information systems.
- By accessing DO information systems, I consent to review and action by authorized Treasury or DO staff. Authorized staff includes my supervisory chain for efficient operation of the workplace as well as systems administrators and information security personnel for



protection of the DO infrastructure. Actions may include monitoring, intercepting, recording, reading, copying, inspecting, restricting access to, blocking, tracking, and disclosing information to authorized Treasury, DO, Treasury Office of Inspector General (OIG) and law enforcement personnel.

- I understand and accept that unauthorized attempts or acts to access, upload, download, change, circumvent, or delete information on DO information systems, modify DO systems, deny access to DO systems, accrue resources for unauthorized use on DO systems, or otherwise misuse DO systems or resources are prohibited.
- I understand that such unauthorized attempts or acts may result in criminal, civil, and/or administrative penalties.
- I will report suspected or identified information security incidents to the DO Help Desk. The DO Help Desk serves as the first tier in incident handling and can be contacted by dialing 202.622.1111 or Helpdesk@treasury.gov.

#### IV. Rules of Behavior

The following ROB applies to employees, interns, contractors and detailees who have access to DO information systems. Personnel are required to exercise “due diligence” and the highest ethical standards to guide all actions in their use of DO information systems.

Personnel must understand that these rules are based on Federal laws, regulations, and Treasury and DO policies. As such, there are consequences for non-compliance with the ROB. Depending on the severity of the violation, at the discretion of management and through due process of the law, consequences can include suspension of access privileges, reprimand, suspension from work, demotion, removal, and criminal and civil penalties. **Failure to agree to this ROB will result in denial of access to DO information assets or resources.**

The following rules apply to all DO users:

As a user of DO information systems I agree that I will abide by all of the following:

- I will follow established Treasury and DO information security and privacy policies and procedures. This includes the requirement to sign the ROB.
- I will only access systems, software, and data which I am authorized to use, and will comply with any applicable copyright restrictions.
- I will use my access for authorized and official duties, and I will only access data that is needed in the fulfillment of my duties.
- I will properly dispose of the information, either in hardcopy, softcopy or electronic format, in accordance with Treasury and DO policies and procedures.
- I will not attempt to override, circumvent or disable operational, technical, or management security controls.
- I will not alter or attempt to alter the configuration on government equipment unless authorized. This includes operational, technical, or management security controls.



- I will comply with the restrictions on personal use of government equipment established by Federal, Treasury, and DO policies and procedures.
- I will not send government-wide or agency-wide broadcast messages unless given explicit authorization.
- I will not transmit sensitive DO or Treasury information to any personal e-mail account, other than through an authorized communication with an individual who is not a Treasury employee.
- I will not copy executable files to any media on a Treasury computer system unless authorized through a formal change control process.
- I will protect passwords/access codes from unauthorized use and disclosure.
- I will not store any passwords/access codes in any type of script file or cache on any DO information system.
- I will log off or lock my assigned workstation before walking away.
- I will not misrepresent, obscure, suppress, or replace a user's identity on the Internet or any DO electronic communication system.
- I will refrain from copying, storing, or maintaining sensitive Treasury information on non-DO equipment or storage devices (e.g., USB drives, CD/DVD, etc.).
- I will not disseminate from DO official equipment or any equipment connected to the DO IT environment, any inappropriate information (i.e. chain letters, games, threatening, obscene, harassing, or personal attacks) through the use of any means of communication including but not limited to email, instant messaging, online chat, web bulletin board, logs, or list servers.
- I will not attempt to connect any personal equipment to a DO network unless explicitly authorized in writing and in compliance with Federal, Treasury, and DO policies.
- I will not attempt to probe computer systems (unauthorized Footprinting) in obtaining information on either available ports or running services for malicious intent.
- I will protect Government property from theft, destruction, or misuse. I will follow Treasury policies and procedures for handling Federal Government IT equipment.
- I will use all virus protection software, anti-spyware, and firewall/intrusion detection software required by the DO on DO equipment or on computer systems that are connecting to any DO network, and will not use additional or different protection or detection software unless authorized by DO.
- I will not disable or degrade tools used by the DO that install security software updates to computer equipment.
- I will complete mandatory security and privacy awareness training within designated timeframes and complete any additional required training for the particular systems to which I require access.



**V. Additional Conditions for Installation or Use of Encryption**

- I will protect sensitive information from unauthorized disclosure, use, modification, or destruction, including using encryption products approved and provided by the DO to protect sensitive data.
- I will only use encryption products as explicitly authorized by the DO. Sensitive data, including but not limited to identifiable information or sensitive financial institution data will only be transmitted using DO-provided encryption capabilities.

**VI. Additional Conditions for Privileged Users**

- I will use my privileged account only for system administration and not to conduct day-to-day business.
- I will complete mandatory specialized security training annually.
- Administrators will not surf or view other personnel's files and folders unless they have been given direct orders to do so by the CIO or the CIO's designee and/or a competent Law Enforcement authority.

**VII. Additional Conditions for Contractors**

- Contractor employees are strictly limited to system or data access necessary to fulfill the terms of the contract. Upon completion or termination of the contract, all contractor equipment used to store DO data shall be sanitized in accordance with Treasury and DO policies.

I acknowledge receipt of the DO ROB. I understand, accept, and will comply with all terms and conditions of this document and the rules of behavior herein. I further agree to comply with any additional Treasury or DO rules of behavior, security alerts, policies, procedures, notices, or directives regarding access to or use of DO data, information systems or resources, upon receipt of such.