Department of Justice
Information Technology (IT) Security
Rules of Behavior (ROB) for General Users
Version 8
January 1, 2015

I. Introduction

These Rules of Behavior (ROB) for General Users pertain to the use, security, and acceptable level of risk for Department of Justice (DOJ) systems and applications. The rules highlight that taking personal responsibility for the security of an information system and its data is an essential part of your job. As a user of the DOJ information technology (IT) data and systems, you are the first line of defense in support of DOJ's IT security.

The intent of the ROB is to acknowledge users' receipt and understanding of applicable IT security requirements from various Federal and DOJ policies and procedures. These requirements include, but are not limited to, the Office of Management and Budget (OMB) Circular A-130, OMB M-07-16, OMB M-05-08, the Privacy Act of 1974, DOJ Order 2640.2 (series), DOJ Order 2740.1 (series), and the DOJ IT Security Standard.

Who is covered by these rules?

These rules apply to all personnel (government employees, interns, and contractors) who have access to information or user accounts that are not privileged on DOJ information systems information, or provide IT services to DOJ—hereafter referred to as users. All users are required to review and provide signature or electronic verification acknowledging compliance with these rules to their respective Component IT Security representative.

When authorized, personnel may obtain limited exemptions from particular terms of these ROB for specific occurrences when necessary to performance of official duties. These individual exemption requests must document why a particular equipment and software rule as reflected in these ROB prevent or hinder mission operations. The system Authorizing Official (AO) will issue an exemption if the accepted risk(s) and justification is documented and appropriate.[1]

In addition to this ROB, users with escalated privileges on a system or application (e.g., administrator) shall also agree to and provide signature or electronic verification acknowledging compliance for the Privileged User ROB.

What are the penalties for noncompliance?

Non-compliance with requirements will be enforced through sanctions commensurate with the infraction. Actions may include a verbal or written warning, temporary suspension of system access or permanent revocation, reassignment to other duties, or termination, depending on the severity of the violation. In addition, activities that lead to or cause disclosure of classified information may result in criminal prosecution under the U.S. Code, Title 18, Section 798, and other applicable statutes.

Unauthorized browsing or inspection of Federal Taxpayer Information (Internal Revenue Code Sec. 7213A) is punishable with a fine of up to $1,000 and/or up to one year imprisonment. Unauthorized

[1] For additional information on mobile device exemptions, please refer to the *Department of Justice Mobile Device and Mobile Application Security Policy Instruction v2* (http://dojnet.doj.gov/jmd/irm/itsecurity/documents/FINAL-DOJ_Mobile_Device_and_Application_Security_Policy_Instruction_v2.pdf).

disclosure of Tax Return information (Internal Revenue Code Sec. 7213) is a felony punishable with a fine of up to $5,000 and up to five years in prison. In addition to these penalties, any Federal employee convicted under Sec. 7213 or Sec.7213A is subject to dismissal from employment.

Users will be held responsible for the compromise of Government information through negligence or a willful act.

II. User Responsibilities

A. General

1. Comply with all Federal laws and Department and Component policies and requirements, including DOJ Orders and Standards. Use DOJ information and information systems for lawful, official use, and authorized purposes only.
2. Ensure that individuals have the proper clearance, authorization, and need-to-know before providing access to any DOJ information.
3. Read and accept the DOJ security warning banner that appears prior to logging onto the system or mobile device.
4. Consent to the monitoring and search of any IT equipment that is brought into, networked to, or removed from DOJ owned, controlled, or leased facilities consistent with employee and contractor consent obtained through log-on banners and DOJ policies.
5. Screen-lock or log off your computer when leaving the work area.
6. Keep your PIVCard on your person when not in use.
7. Do not generate, view, download, store, copy, or transmit offensive or inappropriate information in any medium, to include e-mail messages, documents, images, videos, and sound files (e.g., graphic violence, pornography, hateful language, etc.).
8. Adhere to Separation of Duties principles. Avoid conflict of interest in responsibilities, roles, and functions within a system or application (e.g., duties of the System Administrator and Information System Security Officer [ISSO] should not be combined).
9. Do not use anonymizer sites on the Internet and bypass the Department security mechanisms designed to protect systems from malicious Internet sites.
10. Do not use Peer-to-Peer (P2P) technology (e.g., Skype, BitTorrent) on the Internet unless the Department's Chief Information Officer (CIO) or designee approves a waiver from the Department policy.
11. Do not post Department information on cloud-based services unless approved by the Component CIO or designee.
12. Do not post Department information for official business on public websites or social media unless explicitly authorized for your official duties (e.g., Public Affairs Office).

13. Do not post information on social media or public websites that allows unauthorized users to infer or obtain non-public information (e.g, system account information, personal identifiable information (PII), project status, etc.).

14. Protect and safeguard all DOJ information commensurate with the sensitivity and value of the data at risk, including encrypting all PII being sent to third parties.

15. Protect and safeguard all DOJ information and information systems from unauthorized access; unauthorized or inadvertent modification, disclosure, damage, destruction, loss, theft, denial of service; and improper sanitization or use.

16. Components shall ensure that all DOJ data on authorized removable media (e.g., thumb drives, removable hard drives, and CD/DVD), laptops, tablets, and mobile devices (e.g., smartphones and netbooks) is encrypted with a Department-approved solution unless the Department's Chief Information Officer (CIO) or designee approves a waiver from the Department policy. For classified environments, follow the procedures required for those networks for data storage and transport.

17. Handle all Department data as Sensitive unless designated as non-Sensitive by the Component Head or Office Director.

18. Report any anomalous or unusual behavior, and discovered or suspected security incidents to your appropriate point of contact (POC) (e.g., Help Desk, Incident Response Representative, Security Manager, Supervisor, or Justice Security Operations Center [JSOC], DOJCert@usdoj.gov).

19. Ensure that you complete any required training in accordance with current Department policies.

B. Classified Systems/Information

20. Do not use portable electronic devices (e.g., smart watches, fitbits, laptops, mobile devices, and removable media except CD-R for music) in SCIFs or areas where classified information processing is authorized.[2]

21. Properly mark and label classified and sensitive documents, electronic equipment, and media.[3]

22. Do not process classified information on an unclassified system.

23. Send classified email only on systems authorized for that purpose and for the highest level of the classified data involved.

24. When in use, operate IT systems only in those areas or facilities certified for the highest

[2] For additional information on authorized use of PEDs when working in spaces authorized to process classified information, please refer to *DOJ Order 2640.2F* (https://portal.doj.gov/sites/dm/dm/Directives/2640.2F.pdf), *SPOM Chapter 8* (http://dojnet.doj.gov/jmd/seps/spom/chapter8.pdf), and *Intelligence Community Directive 503* (http://www.dni.gov/files/documents/ICD/ICD_503.pdf).

[3] For additional instruction on proper markings, please refer to the *DOJ Security Program Operating Manual (SPOM)* (http://dojnet.doj.gov/jmd/seps/spom.html).

classification or sensitivity level of the information involved. When not in use, store classified items in an approved security container or in a facility approved for open storage.

25. Only use classified removable media upon approval and after receiving training. Only use it to move data across security domains when an approved Cross-Domain solution is not available and authorization has been given.[4]

C. Passwords

26. Change the default password upon receipt from a system administrator.
27. Do not share account passwords with anyone.
28. Avoid using the same password for multiple accounts.

D. Hardware

29. Do not add, modify, or remove hardware, or connect unauthorized accessories or communications connections to DOJ IT resources unless specifically authorized.
30. Do not access the internal components of the computer, or remove the computer or its hard drive from DOJ facilities, unless specifically authorized.
31. There is no expectation of maintaining any personal information, data, or applications on devices.

E. Software

32. Do not copy or distribute intellectual property without permission or license from the copyright owner (e.g., music, software, documentation, and other copyrighted materials). Use DOJ-licensed and authorized software only.
33. Do not install or update any software unless specifically authorized. Submit requests for system changes through the appropriate help desk or configuration management process.
34. Do not attempt to access any electronic audit trails that may exist on the computer unless specifically authorized.
35. Do not change any configurations or settings of the operating system and security-related software, or circumvent and test the security controls of the system unless authorized through the documented configuration management procedures.

F. Email Use

36. Limit distribution of e-mail to only those with a "need to know."

[4] For additional information on removable media, please refer to the *DOJ Removable Media Requirements for Classified Systems* (http://dojnet.doj.gov/jmd/seps/pdf/removable_media_requirements.pdf).

37. Do not open e-mails from suspicious sources (e.g., people you don't recognize, know, or normally communicate with) and do not visit untrusted or inappropriate websites (unless authorized). Only download permissible files from known and reliable sources and use virus-checking procedures prior to file use.

38. Do not auto-forward emails from your DOJ email account to or through a non-DOJ email system (e.g., Gmail, Yahoo, Outlook.com).

G. Mobile Computing and Remote Access[5]

39. Use mobile Government Furnished Equipment (GFE) (e.g., laptop, tablet, smartphone) for official business and authorized use in accordance with the de minimus rule. Mobile GFE is for use by DOJ personnel only and shall only connect to DOJ networks through an approved DOJ remote access method.

40. Keep all GFE mobile devices assigned to you in your physical presence whenever possible. Secure all of your portable electronic devices and removable media, preferably out-of-sight (e.g. in a locked container) when you are away from the device.

41. Do not bypass native mobile device operating system controls to gain increased privileges (e.g., jailbreaking or rooting the device).

42. Only download and/or install authorized applications and software for mobile GFE on DOJ devices, and only from DOJ-authorized sources.

43. Only install DOJ-provided removable media, including memory (such as SD cards) and subscriber identity module (SIM) cards, on mobile GFE.

44. Immediately report lost or stolen devices (e.g., laptop, phone, tablet, thumb drive) to your appropriate POC (e.g., Help Desk, Incident Response Representative, Security Manager, Supervisor, or JSOC [DOJCert@usdoj.gov]).

45. Do not associate a personal gift or credit card with a government app store account (e.g., iTunes or Google Play). Authorized mobile application purchases should be made by the appropriate contracting officer or official designee (e.g., government purchase card holder).

46. **Unless explicitly authorized by the Authorizing Official (AO) for mobile devices**, follow these rules:

    a. Do not use Short Message Service (SMS) to conduct official government business.
    b. Do not connect non-DOJ mobile devices and/or accessories to DOJ networks, including wireless access.

[5] For additional information, please refer to the *Department of Justice Secure Use of Wireless Networks FAQ* (http://dojnet.doj.gov/jmd/irm/itsecurity/ises_team.php) or the *DOJ Mobile Device and Mobile Application Security Policy Instruction* (http://dojnet.doj.gov/jmd/irm/itsecurity/documents/FINAL-DOJ_Mobile_Device_and_Application_Security_Policy_Instruction_v2.pdf).

c. Do not enable mobile device tethering via Bluetooth, Universal Serial Bus (USB), or wireless hotspots on mobile GFE. If authorized, do not tether between GFE and non-GFE devices.
d. Do not use non-Government-approved cloud-based services (e.g., DropBox and iCloud) on mobile GFE or to transfer DOJ data.
e. Do not connect mobile GFE to non-DOJ information systems, to include personal computers.

47. Follow your organization's telework guidelines when working remotely and/or accessing DOJ information remotely.

48. Ensure the confidentiality of government information when using remote access (e.g., OWA, DOJ Connect, etc.) from a non-GFE client (public or private). This includes the following:

    a. Maintain a reasonable security posture on non-GFE registered/watermarked devices and computers (e.g., updated antivirus, local firewall, updated OS and software patch levels).
    b. When downloading attachments or files to registered non-GFE private computers, immediately remove any extraneous attachments, encrypt them locally, or transfer them to an approved encrypted USB drive.
    c. Delete attachments and files when finished on registered non-GFE private computers.
    d. Do not download attachments or files on unregistered non-GFE public computers.
    e. Do not print emails in public areas and with public non-GFE printers. Users may print with non-GFE private printers at home.

H. Virtual Conferencing

49. Hosts and presenters must provide participants with advance notice if the virtual conference session is being recorded.

50. Do not access a virtual conference presentation using a privileged user account.

51. Limit presentation information to only that which is authorized for dissemination.

52. Delete all DOJ information on a provider's web site immediately upon the end of a virtual conference.

53. Do not install any agents or other software designed to enhance or aid in virtual conferencing. Submit requests for system and software changes through the appropriate help desk or configuration management process.

54. Employ strong participant authentication mechanisms (e.g., multi-factor authentication, creating a pin, unique login credentials).

55. Enable logging and archiving to provide auditability of participant and host activity, as well as enable/disable meeting functions (e.g., upload, download, desktop sharing).

I. Traveling Users

56. Adhere to the Department requirements and recommendations, when possible, regarding foreign travel and mobile devices and laptops in the *DOJ Mobile Device Foreign Travel Security Policy*

Instruction.[6]

57. Your Component CIO/AO, or equivalent, shall notify the appropriate Component POC in advance of foreign travel with the dates and location(s) of travel when you intend to bring a mobile device to a General-Risk country. Your Component POC will then notify JSOC (DOJCert@usdoj.gov). The DOJ Chief Information Security Officer (CISO) must approve the use of laptops for any foreign travel and mobile devices to countries designated as high-risk.[7]

58. Minimize the information on your IT system to what is required to perform a particular mission while travelling and destroy copies of sensitive data when no longer needed.

59. Shut down IT devices when not in use or no longer needed. If the IT device is needed but not the associated network capability, turn off/disable the network/wireless network functionality.[8]

60. Assume all communications (including cellular services) are being intercepted and read when on travel in a foreign country.

61. Keep your remote access token separate from the laptop/tablet (preferably on you) when possible.

J. Personally Identifiable Information

62. Verify that each computer-readable data extract containing sensitive PII data has been erased within 90 days of origination or that its use is still required.

63. Safeguard against breaches of information involving PII, which refers to information that can be used alone or combined with other information that can distinguish or trace an individual's identity—such as a name, social security number, biometric records, the date and place of birth, mother's maiden name, etc.

64. Report all breaches of information involving PII to JSOC through your Component's standard procedures.

65. Access, maintain, store, or transmit PII that you are given explicit authorization to and ensure you meet required security controls.[9]

66. Disclose PII in accordance with appropriate legal authorities and the Privacy Act of 1974.

67. Dispose of and retain records in accordance with applicable record schedules, National Archives

[6] For additional information on traveling with a mobile device, please refer to the *DOJ Mobile Device Foreign Travel Security Policy Instruction* (http://dojnet.doj.gov/jmd/irm/itsecurity/documents/mobile-dev-foreign-travel-sec-pol-ins.pdf).
[7] For additional information on foreign travel requirements, please refer to the *DOJ IT Resources Outside U.S. Territory Waiver Request* form (http://dojnet.doj.gov/jmd/irm/itsecurity/documents/foreign-travel-it-res-form.pdf).
[8] For additional information, please refer to the *Department of Justice Secure Use of Wireless Networks FAQ* (http://dojnet.doj.gov/jmd/irm/itsecurity/ises_team.php).
[9] For additional guidance on PII, please refer to *Information Technology Security, DOJ Order 2640.2F* (https://portal.doj.gov/sites/dm/dm/Directives/2640.2F.pdf).

and Records Administration guidelines and Department Policies.[10]

68. Do not perform unauthorized querying, review, inspection, or disclosure of Federal Taxpayer Information.[11]

III. Statement of Acknowledgement

I acknowledge receipt and understand my responsibilities as identified above. Additionally, this acknowledgment accepts my responsibility to ensure the protection of PII that I may handle. I will comply with the DOJ IT Security ROB for General Users, Version 7.1, dated October 1, 2014.

Signature	Date
Printed Name	Component and Sub-Component

Note: Statement of acknowledgement may be made by signature if the ROB for General Users is reviewed in hard copy or by electronic acknowledgement if reviewed online. All users are required to review and provide their signature or electronic verification acknowledging compliance with these rules. Users with privileged accesses and permissions shall also agree to and sign the ROB for Privileged Users. If you have questions related to this ROB, please contact your Help Desk, Security Manager, or Supervisor.

The Department has the right, reserved or otherwise, to update the ROB to ensure it remains compliant with all applicable laws, regulations, and DOJ Standards. Updates to the ROB will be communicated through the Department's ISES Team Lead and Component Training Coordinators.

[10] For disposal guidance, please refer to *Records Management, DOJ Order 2710.11* (https://portal.doj.gov/sites/dm/dm/Directives/2710.11.pdf).
[11] For additional information on disclosure of federal taxpayer information, please refer to *Internal Revenue Code Sec. 7213 and 7213A (http://www.irs.gov/irm/part11/irm_11-003-001.html#d0e176).*