Department of Justice (DOJ)
Cybersecurity and Privacy
Rules of Behavior (ROB) for General Users
Version 12
January 1, 2019

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. Each DOJ user is responsible for helping to ensure the security and privacy of DOJ information systems and data. As a user of the DOJ information systems and data, each user serves as the first line of defense in support of DOJ's cybersecurity protections and enforcement of appropriate privacy protections of Personally Identifiable Information (PII).

The intent of this ROB is to acknowledge receipt and understanding by DOJ users of applicable cybersecurity requirements and responsibilities (as detailed in 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-17-12, OMB M-16-24, the Privacy Act of 1974, DOJ Order 0904 Cybersecurity Program, DOJ Order 0601 Privacy and Civil Liberties, DOJ Order 2740.1 (series), and the DOJ Cybersecurity Standard.

Who is covered by these rules?

These rules apply to all personnel (government employees, interns, and contractors) who have logical access to DOJ information on DOJ information systems or provide information 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 cybersecurity representative.

When authorized, users may obtain limited exemptions from particular terms of these ROB for specific occurrences when necessary for performance of official duties. These individual exemption requests must document why a particular rule prevents or hinders mission operations. The information system Authorizing Official (AO) has the ability to issue an exemption if the accepted risk(s) and justification are appropriate, substantiated and documented.[1]

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

Users will be held responsible for compromising Government information through negligence or willful acts. Users must use caution and follow all statutory and regulatory access, use, maintenance, and disclosure restrictions, as well as adhere to Department and Component level policies regarding the exchange of access-restricted information such as taxpayer, personally identifiable, controlled unclassified, and grand jury information. Failure to comply with the rules and responsibilities listed in this ROB may result in appropriate sanctions, including but not limited to: remedial training; loss of access to

[1] For additional information on mobile device exemptions, please refer to the *Department of Justice Mobile Device and Mobile Application Security* (https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/2-DOJ_Policy_Instruction/Mobile-Device-Mobile-Appl-Sec-Supp-2017A.pdf).

information; loss of a security clearance; verbal or written warning; termination of employment; or civil or criminal prosecution.

II. User Responsibilities

A. General

1. Comply with all Federal laws and Department and Component policies and requirements, including DOJ Orders, Policy Statements, and Standards. Use DOJ information and information systems for lawful, official use, and authorized purposes only.

2. Ensure 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. Acknowledgment of this ROB also indicates consent to monitoring, recording, and collection of data on all DOJ devices for law enforcement purposes.

4. Consent to the monitoring and search of any IT equipment brought into, networked to, or removed from DOJ owned, controlled, or leased facilities consistent with employee and contractor consent obtained through logon banners and DOJ policies.

5. Screen-lock or log off, and remove the personal identity verification (PIV) card from your computer when leaving the work area.

6. Always keep your PIV card secure. When not in use for authentication and when away from the work area, keep your PIV card on your person and out of sight.

7. Do not generate, view, download, store, copy, or transmit offensive or inappropriate information in any DOJ medium, to include email messages, documents, images, videos, and sound files (e.g., graphic violence, pornography, hateful language, etc.), unless authorized for official purposes.

8. Do not access continuous data streams such as viewing streaming video or listening to streaming audio/radio on a website (e.g., Youtube, Netflix, Spotify) on Department computers and computer systems during working or nonworking hours, unless authorized for official purposes.

9. 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 Database Administrator should not be combined).

10. Do not use anonymizer sites on the internet and bypass the Department security mechanisms designed to protect systems from malicious internet sites unless authorized for official purposes.

11. Do not use Peer-to-Peer (P2P) technology (e.g., BitTorrent) on the internet unless the Department's Chief Information Officer (CIO) or designee approves a waiver from the Department policy.

12. Do not post Department information on cloud-based services unless approved by the Component CIO or designee.
13. Do not use cloud-based services that have not been approved for use by the Department (e.g., DropBox, iCloud, Google Drive/Docs); use the Department's approved file sharing solutions (e.g., Justice Enterprise File Sharing)
14. Do not post Department official business information on public websites or social media unless in accordance with applicable Departmental and Component level policies and explicitly authorized for your official duties (e.g., Public Affairs Office).
15. Do not post information on social media or public websites which allows unauthorized users to infer or obtain non-public information (e.g., system account information, sensitive personally identifiable information (PII), project status, etc.).
16. Upload only the user's picture as a profile picture in Outlook. User's picture must be in a professional pose from the shoulders up with the U.S. flag or a neutral background.
17. Protect and safeguard all DOJ information commensurate with the sensitivity and value of the data at risk, including encrypting all sensitive PII (as defined below) before sending to third parties outside of DOJ.
18. 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.
19. 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 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.
20. Handle all Department data as Sensitive unless designated as Non-Sensitive by the Component Head or Office Director.
21. Report any anomalous or unusual behavior, and discovered or suspected security incidents to an appropriate point of contact (POC) (e.g., Help Desk, Incident Response Representative, Security Manager, Supervisor, or Justice Security Operations Center (JSOC), jsoc@usdoj.gov).
22. Ensure that you complete any required training in accordance with current Department policies.
23. Follow all Department level and Component level policies related to user responsibilities for the recording of information into the Department's recordkeeping systems, and comply with applicable records retention schedules.

B. Classified Systems/Information

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

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

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

26. Send classified email only on systems or authorized devices with the appropriate level of security classification.

27. Operate information systems only in areas certified for the highest classification or sensitivity level of the information being processed. When not in use, classified items should be stored and contained in an approved security facility.[4]

28. Receive the proper security training before handling classified removable media. Transport classified removable media only when authorized.

C. Passwords

29. Comply with Department and Component password policies (e.g, must be at least 12 characters, contains upper-case, lower-case, numeric, and special characters (e.g. ~ ! @ # $ % ^ & * ( ) _ + = - ‘ [] / ? > <)).

30. Change the default password upon receipt from a system administrator.

31. Do not share account passwords with anyone.

32. Avoid using the same password for multiple accounts.

D. Hardware

33. Do not add, modify, or remove hardware, or connect unauthorized accessories or communications connections to DOJ resources unless specifically authorized.

34. Do not access the internal components of the computer or its hard drive from DOJ facilities, unless specifically authorized.

E. Software

[2] For additional information on authorized use of PEDs when working in spaces authorized to process classified information, please refer to *DOJ Order 0904* (https://portal.doj.gov/sites/dm/dm/Directives/0904.pdf), DOJ Security Program Operating Manual (*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)* (https://dojnet.doj.gov/jmd/seps/spom.php).

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

35. Do not copy or distribute protected intellectual property without permission or license from the copyright owner (e.g., music, software, documentation, and other copyrighted materials). Use only DOJ-licensed and authorized software.

36. Do not install or update any software unless specifically authorized. Submit requests for system changes through the appropriate help desk or configuration management process.

37. Do not attempt to access any electronic audit trails that may exist on the computer unless specifically authorized.

38. 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

39. Limit distribution of email only to those who are authorized and need to know the information to perform their job duties.

40. Do not open emails from suspicious sources (e.g., people you do not recognize, know, or normally communicate with) and do not visit untrusted or inappropriate websites, unless authorized for official purposes. Download permissible files only from known and reliable sources and use virus- checking procedures prior to file use.

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

42. Comply with DOJ Policy Statement 0801.04, Electronic Mail and Electronic Messaging Policy Statement, on the appropriate capture of email.

43. Do not use personal email accounts for DOJ business except under exigent circumstances and in accordance with Policy Statement 0801.04, Electronic Mail and Electronic Messaging Policy Statement, and any Component-level policy related to the use of personal email accounts.

G. Mobile Computing and Remote Access[5]

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

45. Always keep GFE mobile devices, portable electronic devices and removable media secure. When not in use, keep GFE mobile devices, portable electronic devices and removable

[5] For additional information, please refer to the *DOJ Mobile Device and Mobile Application Security Policy* (https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/2-DOJ_Policy_Instruction/Mobile-Device-Mobile-Appl-Sec-Supp-2017A.pdf).

media in your physical presence and out of sight.

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

47. Download and/or install only authorized applications and software on DOJ mobile devices, and only from DOJ-authorized sources.

48. Update all mobile devices, including applications and operating systems (e.g., iOS 12 .1. 3 +) to the latest versions and in the timely manner.

49. Install DOJ-provided removable media, including memory (such as SD cards) and subscriber identity module cards, only on GFE mobile devices.

50. 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 (jsoc@usdoj.gov)).

51. 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).

52. **Unless explicitly authorized by the AO for mobile devices**, follow these rules:

    a. Do not connect non-DOJ mobile devices and/or accessories to DOJ networks, with the exception of Guest Networks.

    b. Do not connect mobile GFE to non-DOJ information systems, to include personal computers.

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

54. Ensure the confidentiality of government information when using remote access from a non-GFE device (public or private). As per the DOJ Strong Authentication Plan,[6] this includes the following:

    a. User must authenticate to a VDI solution with an approved LOA-4 credential. [7][8]

    b. Device cannot be joined to the DOJ network domain via VPN.

[6] https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/2-DOJ_Policy_Instruction/doj-strong-authentication-plan.pdf
[7] PIV card readers must be tested and approved by GSA, and therefore listed on the Approved Products List on the Federal ICAM site - https://www.idmanagement.gov/IDM/IDMFicamProductSearchPage
[8] Procurement of PIV card readers must comply with DOJ Procurement Guidance (PGD) 14-03

H. Virtual Conferencing

55. Hosts and presenters must provide participants with advance notice if the virtual conference session is being recorded.
56. Do not access a virtual conference presentation using a privileged user account.
57. Limit presentation information to only that which is authorized for dissemination.
58. Delete all DOJ information on a provider's web site immediately upon the end of a virtual conference.
59. 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.
60. Employ strong participant authentication mechanisms (e.g., multi-factor authentication, PIN creation, unique login credentials).
61. Users are provided with logging, auditing, and the appropriate/authorized meeting functions (e.g., upload, download, desktop sharing).

I. Traveling Users

62. Adhere to the Department requirements and recommendations regarding foreign travel and mobile devices in the *DOJ Mobile Device and Mobile Application Security Policy*.[9]
63. 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 (jsoc@usdoj.gov). The DOJ Chief Information Security Officer must approve the use of laptops for any foreign travel and mobile devices to countries designated as high-risk.[10] The user's Component CIO/AO, or equivalent, shall notify the appropriate Component POC (in advance) of foreign travel. Dates and location(s) of travel will be provided for when the user intends to bring a mobile device to a general-risk country. The user's Component POC will then notify JSOC (jsoc@usdoj.gov). The DOJ Chief Information Security Officer (CISO) must approve the use of laptops and mobile devices in countries designated as high- risk.
64. Inspect computers, smartphones, and any other media that have been transported outside the United States for compromise prior to any physical or logical connection to any DOJ system.

[9] For additional information on traveling with a mobile device, please refer to *the DOJ Mobile Device and Mobile Application Security Policy* (https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/2-DOJ_Policy_Instruction/Mobile-Device-Mobile-Appl-Sec-Supp-2017A.pdf).
[10] For additional information on foreign travel requirements, please refer to the *DOJ IT Resources Outside U.S. Territory Waiver Request* form (https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/2-DOJ_Policy_Instruction/foreign_travel_it_resources_1_2.pdf).

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

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

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

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

J. Personally Identifiable Information (PII)

69. TRAINING:

    a. Complete mandatory privacy training as part of the on-boarding process and annually thereafter, as required by and within the timeframe set by applicable component policy.

    b. Complete role-based privacy training as required by applicable policy, including when the staff member performs specialized privacy roles and responsibilities.

    c. Complete Cybersecurity Awareness Training or similar security training at least annually.

    d. Adhere to all PII training and procedures that are specific to your position.

70. NO EXPECTATION OF PRIVACY:

    a. Know that DOJ information systems include computers, computer networks, and all devices and storage media attached to a(n) DOJ network or to a computer on such network.

    b. Understand and consent to having no expectation of privacy regarding any communications transiting, stored on, or traveling to or from DOJ information systems.

    c. Understand and consent that the Government routinely monitors communications occurring on DOJ information systems for any lawful government purpose including, but not limited to, monitoring network operations, quality control, employee misconduct investigations, law enforcement investigations, and counterintelligence investigations.

    d. Understand and consent that, at any time, the Government may for any lawful government purpose monitor, intercept, search, and seize communications or information transiting, stored on, or traveling to or from DOJ information systems.

    e. Understand and consent that any communications or information transiting, stored on, or traveling to or from DOJ information systems may be disclosed or used for any lawful government purpose.

71. COLLECTION OF PII:

    a. Know that "PII" means information that can be used to distinguish or trace an individual's

identity, either alone or when combined with other information that is linked or linkable to a specific individual. PII can be in any medium or form, including paper, oral, and electronic.

b. Limit the collection of PII to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of your responsibilities.

c. Know that Social Security numbers (SSNs) are singular personal identifiers, and their use poses unique privacy risks, including the risk of identity theft. Special procedures apply to the collection, use, and disclosure of SSNs in some instances; for example, you need to coordinate any disclosure of SSNs outside DOJ with your Senior Component Official for Privacy (SCOP)[11] to ensure that such disclosure is authorized by law. See DOJ Memo on *Minimizing the Use and Disclosure of Social Security Numbers and Protecting Personally Identifiable Information in Motion* (2012).

d. Collect no information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the information is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.

e. Follow applicable Department and Component-level policies related to responsibilities for the recording or inputting of information into the Department's official recordkeeping systems.

72. ACCESS AND USE OF PII: Limit the access and use of PII to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of your responsibilities.

73. MAINTENANCE OF PII:

a. Protect and safeguard PII from loss, compromise, or unauthorized access commensurate with the sensitivity and value of the information and applicable policy. For example, encrypt Social Security numbers when sending via email to any email address outside of the Department.[12]

b. Comply with applicable records retention schedules including requirements to destroy, delete, or purge information, and requirements to preserve or produce it.[13]

c. Use only authorized and appropriate techniques to erase, delete, or purge PII, or dispose of media containing PII.

d. Do not use personally owned information technology such as computers or removable

[11] List of all the DOJ SCOPs: https://dojnet.doj.gov/privacy/scop.php
[12] See Department policy memoranda from DOJ CIO and CPCLO regarding protecting PII and sensitive PII at https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/4-DOJ_%20IT_Memoranda/Data_Loss/Safeguarding%20PII%20Memo.pdf, and https://dojnet.doj.gov/privacy/docs/safeguarding-sens-pii.pdf.
[13] For disposal guidance, please refer to Record Management, DOJ Order 0801 (https://portal.doj.gov/sites/dm/dm/Directives/0801.pdf).

media to store government related work or Department PII.

74. DISCLOSURE OF PII[14]

a. When considering whether to disclose PII (including PII within emails) to a DOJ recipient, ensure the recipient has a need-to-know that information to perform his or her job duties, and that such sharing complies with DOJ policy and the law.

b. When considering whether to disclose PII (including PII within emails) to a non-DOJ recipient, follow applicable DOJ and/or component policy and the law, which may also involve keeping an accounting of the date, nature, and purpose of the disclosures, and the name and address of the person or agency to whom the PII is disclosed. Need-to-know may not be sufficient justification, by itself, for PII disclosure to a non-DOJ recipient.

c. Disclose PII to members of the public including individuals or the media only as allowed by the scope of duties, applicable DOJ and/or component policy, and the law.

d. Do not post information, including PII, on any social media or public website that allows unauthorized user(s) to infer or obtain non-public information.

75. BREACH:

a. Know a "breach" is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose.

b. Report all suspected or confirmed breaches of PII to your supervisor and component-level Security Operations Center or DOJ Justice Security Operations Center (jsoc@usdoj.gov) as applicable, as soon as possible without unreasonable delay, but no later than 1 hour after discovery, and consistent with DOJ Instruction 0900.00.01, *Reporting and Response Procedures for a Breach of Personally Identifiable Information.*

[14] For additional guidance on PII, please refer to Cybersecurity Program, DOJ Order 0904 (https://portal.doj.gov/sites/dm/dm/Directives/0904.pdf) and Privacy and Civil Liberties, DOJ Order 0601 (https://portal.doj.gov/sites/dm/dm/Directives/0601.pdf).

III. Statement of Acknowledgement

I acknowledge receipt and understand my responsibilities as identified above. Additionally, I acknowledge my responsibility to access, collect, use, maintain, and protect PII in accordance with these rules of behavior and applicable laws, regulations, and policies. I will comply with the DOJ Cybersecurity and Privacy ROB for General Users, Version 12, dated January 1, 2019. I acknowledge that failure to comply with the ROB may result in appropriate sanctions, including but not limited to: remedial training; verbal or written warning; loss of access to information systems; loss of a security clearance; termination of employment; or civil or criminal prosecution.

Signature	Date
Printed Name	Component and Sub-Component

Note: Statements 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 Training Team Lead and Component Training Coordinators.