(2 8 6 $ Division MEGA4 Automated Litigation Support System
Account Request and Approval Form
For (2 8 6 $ Division Users

To be used for DOJ (2 8 6 $ Division employees and authorized
0 (* $ FRQWDFWRUVWDII

&DVH 3 URMHFW,QIRUP DWLRQ

DJ NUMBER: 2442-0129

CASE NAME: US v. Epstein

LEAD (2 8 6 $ DIVISION ATTORNEY NAME AND PHONE NUMBER:
[redacted]

(2 8 6 $ CASE MANAGER NAME AND PHONE NUMBER:
[redacted]

☐ iCONECT ☑ RELATIVITY

LIST OF SPECIFIC CASES/PROJECTS FOR WHICH ACCESS IS REQUIRED:
US v. Epstein

End User Information:

FULL NAME:	**EOUSA SECTION:**
POSITION/TITLE:	**TELEPHONE NUMBER:**
BUILDING/LOCATION:	**EMAIL ADDRESS:**

APPROVED BY [redacted] **Date:**

6,* 1 $ 7 8 5 (

Department of Justice
Information Technology (IT) Security
Rules of Behavior (ROB) for General Users
Version 7.0
January 3, 2014

I. Introduction

The Rules of Behavior (ROB) for General Users pertain to the use, security, and acceptable level of risk for Department of Justice (DOJ) systems. 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 and contractors) who perform general non-privileged duties on DOJ information systems, access or use DOJ 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.

Certain authorized personnel may obtain limited exemptions for specific occurrences when performing official duties. These individuals must document situations where equipment and software limitations listed below prevent mission operations. In addition to this ROB, the user shall also agree to and provide signature or electronic verification acknowledging compliance for the Privileged User ROB. The system Authorizing Official (AO) will issue an exemption if the accepted risk(s) and justification is documented and appropriate[1].

What are the penalties for noncompliance?

Non-compliance with requirements will be enforced through sanctions commensurate with the level of 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 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 will be dismissed from employment.

[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).

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. Do not generate, download, store, copy, or transmit offensive or inappropriate information in any medium, to include e-mail messages, documents, images, videos, and sound files.
3. Limit distribution of e-mail to only those with a "need to know."
4. 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.
5. Protect and safeguard all DOJ information, including personally identifiable information (PII), commensurate with the sensitivity and value of the data at risk. Protect and safeguard all DOJ information and information systems from unauthorized access, unauthorized or inadvertent modification, disclosure, damage, destruction, loss, theft, denial of service, improper sanitization, and improper use.
6. 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.
7. Upon discovery of a known or suspected security incident, report the incident to your Help Desk, Incident Response Representative, Justice Security Operations Center, Security Manager, or Supervisor.
8. Immediately report lost or stolen devices (e.g., laptop, phone, tablet, thumb drive) to your Help Desk, Incident Response Representative, Justice Security Operations Center, Security Manager, or Supervisor.
9. Encrypt all DOJ Sensitive but Unclassified (SBU) data on authorized mobile computers, laptops, tablets, and removable media (e.g., removable hard drives, thumb drives, and DVDs) using Department-approved solutions unless a waiver or policy exemption exists. For classified environments, follow the procedures required for those networks for data storage and transport. All data is considered sensitive unless designated as non-sensitive by the Component Director/Head/Office Head.
10. Read and understand the DOJ security warning banner that appears prior to logging onto the system or mobile device.
11. Screen-lock or log off your computer when leaving the work area, and remove your PIV card, if utilized. Log off when departing for the day.
12. Keep all government-furnished equipment (GFE) mobile devices assigned to you in your

physical presence whenever possible. When it is necessary for you to be away from your GFE, particularly at a non-secure location, secure all your portable electronic devices and removable media, preferably out-of-sight (e.g. in a locked container).

13. Do not use Peer-to-Peer (P2P) technology on the Internet, such as Skype, BitTorrent, etc. P2P is forbidden throughout the Department unless the Department's Chief Information Officer (CIO) or designee approves a waiver.
14. Do not auto-forward emails from your DOJ email account to your personal email account (e.g., Gmail, Yahoo, Hotmail).
15. Ensure that individuals have the proper clearance, authorization, and need-to-know before providing access to any DOJ information.
16. Consent to 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.
17. Properly mark and label classified and sensitive documents, electronic equipment, and media in accordance with the DOJ Security Program Operating Manual (SPOM) and DOJ Order 2620.7.
18. Adhere to Separation of Duties principles. Understand 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).
19. 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.
20. Do not bypass native mobile device operating system controls to gain increased privileges (i.e., jailbreaking or rooting the device).
21. Do not use anonymizer sites on the Internet and bypass the Department security mechanisms designed to protect systems from malicious Internet sites.

B. Classified Systems/Information

22. Do not process classified information on an unclassified system unless authorization is obtained to support a specific job function.
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 classification or sensitivity level of the information involved. When not in use, store a classified computer, hard drive, removable media, etc. in an approved security container or in a facility approved for open storage.
25. Use classified laptops and similar devices in accordance with the DOJ Removable Media Requirements for Classified Systems, dated April 25, 2011.

C. Passwords

26. Adhere to at least the minimum password requirements for the system on which you are working.
27. Change the default password upon receipt from system administrator.
28. Do not share account passwords with anyone.
29. Avoid using the same password for multiple accounts.

D. Mobile Computing & Remote Access Users

30. Use mobile GFE (e.g., laptop, tablet, smartphone) for official business and authorized uses. Mobile GFE is for use by DOJ personnel only (no spouses or relatives) and shall only connect through an authorized DOJ remote access network when accessing the Internet.
31. Only authorized applications and software for mobile GFE can be downloaded and installed on DOJ devices, and only from DOJ-authorized sources.
32. The use of Short Message Service (SMS) must be approved by the Authorizing Official. SMS messages are be limited to non-sensitive information.
33. Only install DOJ-provided removable media, including memory and subscriber identity module (SIM) cards, on mobile GFE.
34. Only connect to secure wireless networks where possible and take precautionary measures to prevent the compromise of DOJ data when insecure wireless networks must be used.[2]
35. Follow these guidelines unless explicitly authorized by the Authorizing Official to do otherwise:
    a. Do not connect non-DOJ mobile devices and/or accessories to DOJ networks. This includes mobile phones, tablets, laptops, Bluetooth devices, and other devices requiring both wired and wireless communication access.
    b. Do not enable mobile device tethering via Bluetooth, Universal Serial Bus (USB), or Wi-Fi hotspots on mobile GFE.
    c. Do not access non-Government cloud-based services—such as DropBox and iCloud—from mobile GFE.
    d. Do not connect mobile GFE to non-DOJ information systems, to include personal computers.

E. Virtual Conferencing

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

[2] For additional information, please refer to the Department of Justice Secure Use of Wireless Networks FAQ at http://dojnet.doj.gov/jmd/irm/itsecurity/ises_team.php.

37. Do not access a virtual conference presentation using an account with elevated privileges.
38. Limit presentation information to only that which is authorized for dissemination.
39. Delete all DOJ information on a provider's web site immediately upon the end of a virtual conference.
40. Do not install any agents or other software designed to enhance or aid in virtual conferencing.
41. Employ strong participant authentication mechanisms (i.e., multi-factor authentication, creating a pin, unique login credentials, etc.).
42. 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).

F. Hardware

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

G. Software

46. Do not copy or distribute intellectual property – including music, software, documentation, and other copyrighted materials – without permission or license from the copyright owner. Use DOJ-licensed and authorized software only.
47. Do not install or update any software unless specifically authorized.
48. Do not attempt to access any electronic audit trails that may exist on the computer unless specifically authorized.

H. Remote Web Access

49. Follow your organization's telework guidelines when working remotely and/or accessing DOJ information remotely.
50. Ensure the confidentiality of government information when using remote web access (e.g., OWA) from a non-GFE client (public or private). This includes the following:
    a. When downloading attachments to registered non-GFE private computers, immediately remove any extraneous attachments, encrypt them locally, or transfer them to an approved encrypted USB drive.
    b. Delete attachments when finished on registered non-GFE private computers.
    c. Do not download attachments on unregistered non-GFE public computers.

51. Do not print emails in public areas and with public non-GFE printers. Users may print with non-GFE private printers at home. Users will be held responsible for the compromise of Government information through negligence or a willful act.

52. Maintain a reasonable security posture (i.e., updated antivirus, local firewall, updated OS and software patch levels) on registered non-GFE private computers used for remote access.

I. Traveling Users

53. The Component Mobile Computing Operations Manager, or equivalent, shall notify the JSOC, or an equivalent authorized SOC in advance, if you intend to travel to a foreign country with a DOJ laptop that will accompany you during any portion of travel with the intended dates and location(s) of travel. For travel to countries designated as high-risk counter-intelligence, the use of mobile devices must be approved by the DOJ CISO prior to travel. Requests are processed via email to both the DOJ ITSS Director and the DOJ ITSS Deputy Director.[3]

54. 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.

55. 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.[4]

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

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

J. Personally Identifiable Information

58. 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.

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

---

[3] For additional information on foreign travel requirements, please refer to the *Foreign Travel Laptop Use* and *Foreign Travel Laptop Use Waiver Request* forms (http://dojnet.doj.gov/jmd/irm/itsecurity/jsoc-cyber-defense.php). For additional information on the use of mobile devices during foreign travel, please refer to the *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).

[4] For additional information, please refer to the Department of Justice Secure Use of Wireless Networks FAQ at http://dojnet.doj.gov/jmd/irm/itsecurity/ises_team.php.

60. Access, maintain, store, or transmit PII that you are given explicit authorization to and ensure you meet required security controls.[5]
61. Disclose PII in accordance with appropriate legal authorities and the Privacy Act of 1974.
62. Dispose of and retain records in accordance with applicable record schedules, National Archives and Records Administration guidelines and Department Policies.[6]
63. Do not perform unauthorized querying, review, inspection, or disclosure of Federal Taxpayer Information.[7] (*See Internal Revenue Code Sec. 7213 and 7213A at http://www.irs.gov/irm/part11/irm_11-003-001.html#d0e176*)

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 7.0, dated January 3, 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 email/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.

[5] 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).
[6] For disposal guidance, please refer to *Records Management, DOJ Order 2710.11* (https://portal.doj.gov/sites/dm/dm/Directives/2710.11.pdf).
[7] 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).*