**UNITED STATES ATTORNEYS'**
**INFORMATION SYSTEMS RULES OF BEHAVIOR**

Access to United States Attorney information systems, and the sensitive law enforcement and other official information they contain, is governed by USAP 3-16.200.003, Network Account Security Management, which requires all users to read and sign these Rules of Behavior (RoB) prior to access. To ensure that all users are aware of periodic RoB revisions, annual recertification will be part of each year's Computer Security Awareness Training.

A. Classification Usage

1. These rules apply to United States Attorneys' information systems used for storing, processing, and transmitting information designated **LIMITED OFFICIAL USE.** Such systems **must not** be used to store, process, or transmit information that has been identified as Top Secret, Secret, or Confidential in accordance with Executive Order 13526, "Classified National Security Information" (December 9, 2009).

B. User ID and Password Management

1. Do not disclose your unique User ID or password under any conditions. You are individually responsible and accountable for protecting your unique User ID and password.
2. Do not write passwords in any form, either electronically (e.g., login scripts) or hardcopy.
3. Do not share your User ID and password. They are individual credentials that are used to establish a single session that is solely under your control and for which you are accountable.
4. Do not establish a session under your ID and password for another user.
5. Once your account has been successfully initialized using an administrator-provided password, immediately change the password.
6. If your password has been compromised, or is suspected of being compromised, change it immediately and report the incident to your Systems Manager and District Officer Security Manager.

C. Computer Hardware

1. Protect Government-owned computer hardware from incidents such as damage, theft, abuse, loss, and unauthorized use, and report any such incidents or suspected incidents to the District Officer Security Manager and Systems Manager.
2. Obtain a property pass if computer hardware has to be removed from USAO or EOUSA premises, except for permanently assigned laptops, portable hard drives, smartphones, and other Government-furnished devices (e.g., iPads).
3. Computer hardware shall not be removed from USAO or EOUSA premises for unofficial purposes.
4. Do not use computer hardware for which you have not been specifically authorized.
5. Hardware maintenance or configuration changes shall only be performed by authorized personnel.
6. Do not connect or use any unauthorized devices with Government-owned computer hardware.

7. Government-owned computer hardware must be handled as carry-on luggage when using airlines, trains or any other common carriers. Do not check in Government-owned computer hardware on any common carriers.
8. Do not leave Government-owned computer hardware unattended in vehicles or in locations that are susceptible to theft. Store Government-owned computer hardware that is not in use in a secure location.
9. Loss or theft of a DOJ laptop, smartphone, removable media (e.g., "thumb" drives), and other Government-furnished devices shall be reported immediately to the District Officer Security Manager and EOUSA Assistant Director for Information Systems Security.

D. Reporting of Security Breaches

1. Report any actual or suspected security violations, incidents, vandalism or vulnerabilities to the District Officer Security Manager and Systems Manager.

E. Work at Home and Other Remote Users

1. Personally-owned (non-governmental) hardware and software may not be used for work purposes, except that users of Government-furnished remote access devices (e.g., High-Speed Remote Access (HSRA), USAConnect USB drives, or Remote Access 2012) may use non-governmental Internet connections to establish remote connections.
2. All of the on-site safeguards for handling SBU information apply to off-site work.
3. Remote access may not be used for purposes other than official business.

F. Computer Software

1. Software Copyright Laws and Licensing Agreements must be honored both for computer programs and documentation.
2. End-users shall not install software on Government-owned computer systems. For ad-hoc software needs, contact your Systems Manager.

G. Property

1. An employee has a duty to protect and conserve Government property and shall not use such property, or allow its use, for other than authorized purposes (5 C.F.R. §2635.704). Government property includes, but is not limited to, DOJ-issued hardware and software.
2. Do not use Government property for personal commercial gain or to promote personal causes or in an attempt to influence legislation or elections.

H. Communications and Usage

1. Do not transmit SBU or other sensitive information, or copyrighted documents over the Internet unless encrypted.
2. Do not auto-forward electronic mail over the Internet.
3. Do not utilize nongovernmental Voice-Over-IP websites, e.g., Skype.
4. Abide by the Standards of Ethical Conduct for Employees of the Executive Branch.
5. Political activity, commercial activity (e.g., conducting a business), unlawful activity, and inappropriate conduct are prohibited.
6. Any personal use must be on personal time, have a negligible cost to the government, and be of reasonable duration.

7. Obtaining, viewing, or transmitting sexually-explicit material is prohibited except for official law enforcement purposes.
8. Do not forward chain letters, jokes, or other inappropriate content.

I. Confidentiality

1. Do not use or attempt to access data for which you have not been authorized.
2. Information that you are authorized to retrieve from information systems is for your use only, and not to be shared.
3. Ensure that sensitive information sent to a fax or printer is handled securely and labeled appropriately (e.g., use a fax cover sheet that indicates the classification and sensitivity of the information, contact information for recipient and sender, and instructions to the recipient if the information is received in error).

J. Integrity

1. Do not introduce unauthorized, inaccurate or false information into information systems.
2. Do not use system privileges to misuse or exploit information in information systems.
3. Do not alter files improperly. If files appear to be altered improperly or are missing, notify your Systems Manager and District Officer Security Manager.

K. Availability

1. Do not eat, drink, smoke, or store combustible materials near a computer or electronic media.
2. In the event of a crash or system outage, check that critical files are available and have not been altered. If files are missing or appear to be altered, notify your Systems Manager and District Officer Security Manager.

L. Hardware and Software Support

1. Do not attempt to perform hardware or software support activities. Contact your Systems Manager and use District procedures for hardware and software support.

M. Additional Provisions for Privileged Users

1. Use non-privileged accounts by default. **Use your privileged accounts only in the performance of official duties and only as necessary to complete assigned tasks.**
2. Do not make unauthorized changes to systems.
3. Do not deploy patches, updates, or upgrades except as authorized via Technical Bulletin or Security Bulletin. Do execute bulletins in accordance with deadlines.
4. Browsing the web, accessing email, or accessing any other Internet resource with a privileged account is prohibited.

I acknowledge that I have read the above Rules of Behavior and understand my responsibilities and agree to comply with the Rules delineated herein. I acknowledge that any violation of these Rules may be cause for disciplinary actions.

Signature: _____ Date: _____

Printed Name: _____