# Rules of Behavior for Computer Network Users Reference Guide

This *Rules of Behavior for Computer Network Users Reference Guide* (the *Guide*) provides additional guidance and examples to help you understand and comply with the *Rules of Behavior for Computer Network Users* (the *Rules*). Both the *Rules* and the *Guide* will help you better understand the due care and diligence that is required to protect Department of the Interior (DOI) information and information systems. The information in the *Guide* is further explained and supported by the required annual *Federal Information Systems Security Awareness + Privacy and Records Management* training and the updated Department Manual Series 17, Part 375, Chapter 19.

If you have any questions regarding the *Rules*, the *Guide*, or related issues, please contact your supervisor.

As a DOI computer network user[1], you are required to:

1. **Successfully complete the initial and annual *Federal Information Systems Security Awareness + Privacy & Records Management* training.**

    - This training provides comprehensive information security, privacy, and records management guidance to ensure that due care is exercised at all times to protect DOI information and information systems.

    - You must complete this training prior to accessing the DOI computer network and annually thereafter. Failure to complete annual training will result in a suspension of your user account(s) until the training is completed.

    - The training may be taken and viewed from the DOI Learn website: http://www.doi.gov/doilearn. DOI Learn requires a DOI-assigned username and password.

2. **Handle and maintain all information and system outputs in accordance with the provisions of the Privacy Act and policies for safeguarding personally identifiable information, information classifications, and records management requirements.**

    - You must be aware that DOI information may be sensitive and must be handled according to its sensitivity level. For example, sensitive, personally identifiable information (PII) must be encrypted when sent via e-mail to individuals outside the

[1] The terms "Government computer equipment", "DOI computer network", "computer system" and similar terms as used in these Rules of Behavior and Reference Guide include all Department-owned or issued hardware and software that is used by, attached to, or sends or receives information through the DOI network, including but not limited to, desktops, laptops, tablets, personal data assistants (PDA's), cell phones, smart phones, flash drives and other storage or communications devices.

Department. BisonConnect already provides encryption for emails sent between DOI user accounts.

- Examples of information that must be protected include, but are not limited to, the following:

  - Personally Identifiable Information (PII) – Any of the following items individually or combined could be considered PII: An individual's name, Social Security Number, home address, home phone number, date of birth, place of birth, mother's maiden name, nationality, or credit card number.

  - Proprietary Data - Trade secrets, copyright data, trademarks or patents.

  - Federal Records - Documents, books, maps, photographs, machine-readable materials, or other documentary materials that agencies create and receive in the course of conducting official business that provide evidence of the agency's organization, functions, policies, decisions, procedures and operations, in any media including paper, tape, electronic, disk or other physical form, which must be preserved and protected against removal, alteration or destruction.

  - Sensitive Information – Any information designated as controlled unclassified information or contains unclassified information markings including network diagrams, building plans, etc., which if not secured could be used to negatively impact DOI networks or facilities, contract information, Indian trust information, any information that may give a group or company an unfair competitive advantage, or any information where the loss, misuse or unauthorized access to or modificaiton of could adversely affect the national interests or conduct of Federal programs, or the privacy to which individuals are entitled to under the Privacy Act.

  - Financial Information - Accounts used to transfer funds for DOI business (not just employee accounts/awards, etc.).

- Examples of best practices to ensure that handling and retention requirements are met:

  - Ensure PII or other sensitive information is secured when not in use.

  - Ensure PII or sensitive information is disposed of in accordance with applicable records schedules, and National Archives and Records Administration guidelines and DOI policy.

  - Immediately pick up sensitive printouts and faxes.

  - Do not automatically forward work emails to an external email address.

  - Do not allow unauthorized access to sensitive data.

  - Do not allow unauthorized persons to overhear discussions of privacy protected information.

  - Never destroy Federal records that are not scheduled for disposition. Contact your Records Officer if you have any questions.

3. **Ensure the security of DOI information, equipment, keys, and DOI Access card.**

- You must protect the government issued devices that you use to store and/or access information. This is especially important while teleworking from any remote location or when traveling.

- Examples of best practices to protect information, equipment, keys and your DOI Access card are:

  - Immediately report stolen, lost or missing government issued equipment, keys, or your DOI Access card to your supervisor and respective HelpDesk personnel for action.

  - Immediately report any suspected or confirmed loss of privacy data or other sensitive information, or any suspected computer security incidents to DOI CIRC (doicirc@ios.doi.gov; 703-648-5655) and your supervisor.

  - Immediately report the loss or destruction of agency records subject to the Federal Records Act to your supervisor and your bureau's records officer. Please see the following site for a list of all bureau records officers: http://www.doi.gov/ocio/people/records-management-contacts.cfm

  - Log off your computer or manually initiate the screensaver lock when stepping away from your computer.

  - Keep your DOI Access card in the shielded card holder to protect the data stored on the card.

  - Store information, portable equipment, keys and your DOI Access card out of sight in a secure location when not in use.

  - Never let an unauthorized individual (family member, friend, etc.), access, and use or borrow DOI information, equipment, keys, or your DOI Access card.

  - Always keep DOI information, equipment, keys and/or your DOI Access card in your control while on travel.

- Never pack information, equipment, keys and/or your DOI Access card in checked-in baggage when traveling.
- Position yourself so that no one else can read information on your computer screen.
- Always lock your office when you are away.

4. **Refrain from attempting to access information or information systems for which access has not been authorized.**

- Examples of unauthorized access attempts include, but are not limited to:
  - Using another user's computer, without authorization, while they are logged into the network.
  - Viewing information on another user's computer screen without authorization.
  - Intercepting and reading other employees' printouts from unattended printers or fax machines.
  - Attempting to access computer folders on the network to which you do not have authorized access (Example – attempting to access another DOI employee's home drive on a file server).

5. **Refrain from sharing passwords and/or your DOI Access card personal identification number (PIN).**

- Your passwords must remain confidential to ensure they remain unique to you. You are responsible for actions taken under your DOI computer account. Each account must be linked to only one DOI employee. Your DOI Access card and PIN can be used to access DOI facilities, computer network and information assets, and digitally sign messages and documents. As such, it is especially important that you protect these items. Never share your DOI Access card PIN with anyone.
- Ways to protect your password and PIN include the following:
  - Never share your passwords or your DOI Access card PIN with anyone.
  - Memorize your passwords and PIN.
  - If you write your passwords and/or PIN down, keep them in a secure place.
  - Never let anyone watch you typing in your password and/or PIN.
  - Never email your passwords and/or PIN to yourself.

    - Never post your password or PIN on your desk, desktop computer or laptop.

6. **Refrain from using DOI information, equipment, keys and/or your DOI Access card for activities that are illegal and/or inappropriate.**

    - Using DOI information systems for illegal or inappropriate activities wastes DOI resources and can introduce computer viruses or malware to the computer network. Additional information regarding inappropriate use can be viewed within the DOI Limited Personal Use of Government Office Equipment and Library Collections policy.

    - Examples of illegal or inappropriate activities include but are not limited to:

        - Viewing or distributing pornography.

        - Gambling.

        - Terrorist activities.

        - Harming or threatening other people.

        - Downloading or sharing copyrighted content, including music, movies, and books.

7. **Consent to monitoring and have no expectation of privacy when using DOI computer equipment and/or the DOI computer network.**

    - You should see the DOI Login Warning Banner every time you log into the DOI computer network. This banner requires all computer network users to agree and consent to the monitoring of the user's computer.

    - The DOI Login Warning Banner reads as follows:

> This computer system, including all related equipment, networks, and network devices (including Internet access), is provided by the Department of the Interior (DOI) in accordance with the agency policy for official use and limited personal use.
>
> All agency computer systems may be monitored for all lawful purposes, including but not limited to, ensuring that use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Any information on this computer system may be examined, recorded, copied and used for authorized purposes at any time.

> All information, including personal information, placed or sent over this system may be monitored, and users of this system are reminded that such monitoring does occur. Therefore, there should be no expectation of privacy with respect to use of this system.
> By logging into this agency computer system, you acknowledge and consent to the monitoring of this system. Evidence of your use, authorized or unauthorized, collected during monitoring may be used for civil, criminal, administrative, or other adverse action. Unauthorized or illegal use may subject you to prosecution.

8. **Refrain from attempting to install unauthorized software onto DOI computers.**

   - Unauthorized software can introduce unwanted computer viruses and malware to the DOI network. Only designated personnel are authorized to install programs on DOI computers.

9. **Refrain from attempting to connect personal devices or other unauthorized computer equipment to the DOI network without appropriate authorization.**

   - Unauthorized computer equipment can introduce viruses and malware to the DOI computer network.

   - Examples of unauthorized computer equipment include, but are not limited to, non-DOI issued:

     - Thumb drives;
     - Laptops and personal computers;
     - Cell phones;
     - Wireless access points;
     - Personal scanners and/or printers;
     - Digital Cameras; and
     - Tablet Devices.

10. **Refrain from posting DOI information on external websites without prior appropriate authorization.**

    - Only authorized personnel are allowed to post DOI information on public websites.

- Examples of websites that may lead to unauthorized information sharing are listed below, but are not limited to:
    - Blogs.
    - Social Networking Sites (MySpace, Facebook, YouTube, Google+, Twitter, etc.).
    - Message Boards.

11. **Refrain from attempting to alter and/or disable DOI computer configurations and security settings without prior appropriate authorization.**

- Your DOI computer was supplied to you with pre-configured settings to protect DOI information. You must not attempt to change any of these computer settings.

- Examples of computer configurations and security settings that should not be altered and/or disabled are listed below, but are not limited to:
    - Antivirus software settings.
    - Computer registry settings.
    - Encryption software settings.

12. **Immediately report suspected computer security incidents, privacy incidents, loss or destruction of Federal records, equipment, keys and/or DOI Access card by following your Department, Bureau, and/or Office incident response procedures.**

- A security incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Any action that breaks any of the above-mentioned rules is a security incident. You must cooperate willingly with official DOI actions during the research of, and response to, security incidents and/or violations.

- A privacy incident is defined as the loss of control, compromise, unauthorized access or disclosure of personally identifiable information, whether suspected or confirmed. You must immediately report privacy incidents and cooperate willingly with official DOI response activities during investigation and remediation of a privacy incident

- Examples of security and privacy incidents include, but are not limited to:
    - Someone requesting your password.
    - The loss of DOI computer equipment.

- Witnessing someone willfully or accidently share sensitive information to unauthorized personnel or the public.

- Physically plugging personal equipment into a DOI provided system that may be connected to the DOI network or directly to the network itself.

- Sending an email containing unencrypted sensitive PII to another agency, organization or person.

- Posting sensitive PII to a shared drive without establishing access restrictions.

- Storing sensitive PII on an unencrypted flash drive.

- Knowingly accessing or viewing PII without authorization.