Use Of OIG Information Technology Resources

This policy covers OIG owned or leased information technology (IT) resources as outlined in Treasury Policy TD P 85-01 Treasury Information Technology Security Program and Treasury Directive TD 87-04 Personal Use of Government Information Technology Resources. IT resources include items such as personal computers, network servers, laptop computers, software applications, IT supplies, telecommunications equipment, and IT services.

What is appropriate use?

You can use OIG IT resources:

- For investigations, audits, evaluations, oversight, management, research, and any other activities required by your job.
- For limited personal use during non-work times (e.g., breaks, lunch or after work) for a reasonable duration.
- If it does not adversely affect the performance of official duties or interfere with the mission or operations of the departments, bureaus, or offices.
- When necessary for OIG work, the Deputy Inspector General or Assistant Inspector General for Management can authorize use that is normally prohibited.

What is inappropriate use?

- Unauthorized creation, downloading, viewing, storage, or transmission of graphics, images, or sound, which are sexually explicit, discriminatory, offensive, obscene, or intended to harass.
- Unlawful or malicious activities prohibited on Federal property. This includes the creation and maintenance of information used in the conduct of a private business.
- Installing, copying, or deleting software without authorization from the Office of Management, Information Technology Division (ITD).
- Exchanging or removing IT resources without ITD authorization. For example, this would include removing a printer from a departing employee's office.
- Visiting internet chat rooms, forwarding chain letters, posting of OIG information to external news groups, bulletin boards, or forums.
- Engagement in matters directed toward the success or failure of a political party, candidate for partisan political office, or partisan political group, or activity to support political fund raising.
- Downloading illegal or unauthorized copyrighted content, including illegal downloads using file sharing programs, and downloading un-trusted, unapproved, or malicious software.
- Downloading, copying, and/or playing of computer video games.
- Viewing, storage, or transmission of materials related to all gambling (legal and illegal), illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited.

May I use somebody else's account to log on the OIG network?

No. Every employee gets a unique network account to access the OIG network. Only use the account assigned to you. Please do not give your password to anyone else.

Why do I see a warning message when I first log on to my computer?

The use of a security message is an important security practice. It lets us know we lack reasonable expectation of privacy when using OIG IT resources. Management can and may monitor all computer use. Inappropriate use can result in disciplinary action. Also, the message may aid the prosecution of intruders.

Can I take government computer equipment home?

Your supervisor can allow you to take a government computer home based on the following criteria:

- You need it to do time sensitive work that cannot be done at your normal duty station.
- You and your supervisor have signed the OIG "Telework" Agreement.
- You understand the equipment cannot be used for "classified" work or by non-OIG employees.
- You understand you may be liable for damages and/or losses resulting from negligence during the transportation and use of OIG IT resources.

- You understand that you are required to encrypt, protect and log sensitive and personal information that is stored on computers or removable devices

May I load software on my government computer?

You may not install personal software on OIG IT resources. Software packages can only be installed with ITD assistance and must be approved by the Director, ITD. To have software installed, please outline the need by email to the IT HelpDesk at Helpdesk@oig.treas.gov and, for software you own, provide license information. You may only reconfigure software and network features for which you have access. Do not attempt to bypass security permissions on OIG IT resources. ITD validates the OIG software inventory to prevent unauthorized software use.

Can I do government work on my privately owned personal computer?

Yes, but only with the approval of the ITD Director and if the computer meets the following criteria:

- There is no processing and/or storage of sensitive, personal, or classified information.
- All government-related information processed by the computer is the property of the government.
- You agree the government is not liable for the computer's loss, destruction, or maintenance.
- You check your computer files for viruses before transferring them to a government computer.

Can I attach and use a personally owned computer or device on the OIG network?

No. Treasury security policy does not allow for personal computers to enter within the firewall. Employees are not allowed to attach or use personally owned equipment on the OIG network for any reason including accessing servers, files or systems.

Who is responsible for the management of IT resources?

The ITD Director, senior managers, program managers, IT liaisons, and employees share responsibility for the proper management of OIG IT resources.

- **The Information Technology Investment Review Board** is composed of the Inspector General, the Deputy Inspector General, the Assistant Inspectors General, and the Chief Information Officer (or their designees).
    - Provides guidance for anticipated IT resources needed in support of major operational initiatives being planned.
    - Reviews, for approval, the short-term and long-term plans for the procurement and use of major IT resources.

- **The ITD Director** has overall responsibility for OIG IT resources management and administration.
    - Resolves conflict for multiple requests of an IT resource in limited supply.
    - Improves OIG operations and realizes savings through the application of up-to-date IT.
    - Evaluates IT products' operational and technical features for OIG applicability.
    - Approves software and hardware modification requests.
    - Designs, develops, tests, and implements IT resources to ensure high quality and cost-effective operations and maintenance of the OIG environment.
    - Develops and provides IT resources training programs and/or recommends suitable sources of training for OIG employees and IT Liaisons, and conducts new employee IT resources orientation.
    - Monitors IT resources use to determine the impact on other IT resources, the need for changes and upgrades, and the existence of any abuses.

- **Senior managers, program managers, and/or subject matter experts** are responsible for the appropriate use of IT resources under their management control.
    - Ensure employees are informed of this Directive and their assigned responsibilities.
    - If necessary, correct employees for inappropriate/prohibited use of IT resources, and report these incidents to the ITD Director for development of preventive measures.
    - Designate primary and alternate IT Liaisons as needed.
    - Designate Property Accountable Officers responsible for tracking IT equipment at their locations. These individuals need to validate the IT resources inventory at least yearly.

- **Information technology liaisons** work with their senior managers and the ITD Director to aid compliance with this Directive for their individual areas.

- Receive and test IT equipment to ensure it works.
- Ensure copies of signed Request for Property Action and Acceptance of User Responsibility sheets are kept locally.
- Verify quarterly the IT resources inventory for his/her area.
- Serve as front-line points-of-contact for the identification of additional IT resources that would be of potential benefit. Report these requirements, along with justifications, to his/her senior manager and to the ITD Director.
- Work with subject matter experts and/or ITD to test and implement new IT resources.
- Assist employees and contractors by providing IT resources support in his/her area.

- **Employees, student interns, and contractors**
  - Maintain the integrity of the OIG's hardware and software.
  - Sign a Request for Property Action sheet for OIG equipment that has been assigned to you.
  - Sign an Acceptance of User Responsibility sheet for use of OIG IT resources.
  - Access only the IT resources and data specifically authorized.

If I have a question about this policy, whom can I contact?

Please contact the Office of Management by email at OIG-OM@oig.treas.gov or call our main line at (202) 927-5200.

Office of the Inspector General GSS Acceptance of User Responsibility

Violations of OIG GSS computer policies or Department of Treasury computer policies may lead to disciplinary action, consistent with the personnel policies and practices of the violator's organization, and, in some cases, criminal prosecution. Signing this form acknowledges your understanding of the requirements for access to the GSS system and your responsibilities regarding appropriate use of the system.

Signatures:

Employee Name: _____
(Print)

Title: _____

Organization: _____

Office Address: _____

_____

Work Phone: _____

E-Mail Address: _____

Employee Signature: _____

Date Signed: _____

Supervisor's Signature: _____

ISSO's Signature: _____

Return completed form to the Office of Management, 740 15th Street NW Suite 510, Washington, DC 20220