OIG Information and Physical Security

This policy addresses OIG information and physical security as outlined in Treasury Policy TD P 85-01 Treasury Information Technology Security Program.

Security is everyone's responsibility and needs to be integrated into our work. By "information security," we mean controlling access to sensitive and personal data, images, documents and files stored in cabinets, desks, boxes, open stacks and on computer equipment, disks, tapes, and removable storage devices. By "physical security", we mean controlling access to our building, work areas and equipment.

What kind of data can I store on OIG computers, servers, and devices?

You may store both non-sensitive and sensitive information on OIG computers, servers, and devices.

Examples of sensitive information include, but are not limited to:

- Personally Identifiable Information (PII) and other Privacy Act-protected information.
- Sensitive But Unclassified (SBU) information.
- Law enforcement information.
- Time and attendance documents.
- Confidential business information such as contractor information.
- Grand Jury information.
- Official use only documents.
- Tax return/taxpayer information.
- Investigative reports and memoranda.
- Audit findings before their official release.

What is PII?

Personally Identifiable Information (PII) is defined by OMB as "any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc."

Can I transfer sensitive information through an email?

Yes. When sending sensitive information via e-mail outside of the OIG, you must use Winzip and its encryption feature. E-mails sent via Outlook are not automatically encrypted when they are sent to Internet addresses. E-mails transmitted via Blackberry are sent in an encrypted form.

What can we do to secure information?

- Do not physically remove or send electronic sensitive information unless it has been encrypted.
- Protect your work areas and equipment.
- Limit access to computers and network resources.
- Defend against computer viruses.
- Do not share your password with anyone.
- Immediately report incidents and security violations.
- Certify that we have secured sensitive information throughout the OIG.
- Participate in OIG information security meetings.

How do we protect sensitive information on my computer or on the network?

- OIG uses a Microsoft Windows security feature called Encrypting File System (EFS) that encrypts and protects sensitive information stored on your hard drive. It encrypts sensitive information so that the data is unreadable if a computer is lost or stolen.
- Maintain backup copies of your data. Information on OIG servers is backed up nightly.

- Secure your floppy / CD / thumb drive and any other removable media when not in use (e.g., in a locked drawer or behind a locked door). When taking removable media outside of the OIG, you must use the Winzip encryption feature.
- Electronically lock your workstation when you leave it or physically lock the room that it is in.
- Log all information extracts from databases and data sources containing PII. You must verify that the extracted data has been erased within 90 days unless it is still required.

How should we protect our work areas and equipment?

- Prevent unauthorized access to your work area and files at all times. Lock up sensitive files and information. Let your supervisor know if you are not able to do this and why. Supervisors have an obligation to help you secure your work area and files.
- Strictly control keys. Have employees sign out and sign in all keys and access cards. Limit the number of master keys circulated.
- Check your door(s) and/or cabinet(s) to make sure they are locked when you leave your work area. Supervisors need to spot check all doors and cabinets during and outside of normal work hours to make sure they are locked.
- Keep unauthorized people away from computers and other network equipment including servers, copiers and printers.
- Be aware of and politely challenge strangers in your area or any OIG office. Make sure that an employee accompanies all visitors or have visitors wear a temporary visitor's pass issued by the OM at Headquarters, or by your building management outside of D.C., if appropriate.

How can we limit access to our computers and network resources?

- "Lock it" for short periods (e.g., to run errands or attend short meetings). Use Ctrl-Alt-Delete, and choose "Lock Computer," your screen saver should automatically lock your screen after 10 minutes of inactivity. If you have questions about these options email the IT Help Desk at Helpdesk@oig.treas.gov
- "Log off" for longer periods such as an off-site meeting or lunch. This closes all of your open applications.
- "Shut Down" for evening departures. This option closes all of your open applications, disconnects you from the network, and shuts down all hardware for the evening.

How can we defend against computer viruses?

- Use your virus software to scan all files and diskettes received from anyone else. Currently, all OIG computers have virus software that does this automatically.
- OIG security policy does not allow users to install software without first getting permission. Software installations may make our network more vulnerable to viruses. The IT Help Desk tests all software packages before installation. If you want to install new software, email the IT Help Desk at Helpdesk@oig.treas.gov.
- Only open email messages and attachments from people and organizations you know. Do not open any that look suspicious; contact the IT Help Desk at Helpdesk@oig.treas.gov when in doubt.

How can we protect our passwords?

- Do not write your password down or give it to anyone.
- Choose hard to guess passwords. Avoid birthdays, kids' names, etc.
- Change your password immediately if you think someone else knows it.
- Use special characters, numbers, or punctuation when creating a password.

Who do we notify to report an incident or security violation?

- Tell your supervisor if you see any unauthorized changes to your data, if you notice unexplained loss of paper or electronic information or suspect unusual computer behavior.
- Lost or stolen computer equipment has the potential to expose sensitive data to unauthorized parties and must be reported immediately to the IT Help Desk at Helpdesk@oig.treas.gov

Do we need to report that we have secured sensitive information in our work areas?

Yes. At least once a year, we will ask the Assistant Inspectors General (AIGs) and Counsel to certify (through the AIG for Management) to the Deputy Inspector General that they have secured information in their work areas. We will do this using a brief but thorough survey.

How does the OIG provide security training to employees?

Completion of the IT Security Awareness course is required on an annual basis. Other information security briefings can also be found online.

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.