

Department of the Interior

<Bureau>

<Office/Organization>

Emergency Response Center

Information Technology Security

Awareness and Best Practices

Multiple laws and policies require that the Department of the Interior (DOI) have an effective and rigorous Information Technology (IT) security awareness program. Security is not just a technical problem—it is also a management and people issue. Without management support and employee cooperation, computer and information security programs cannot be successful.

The difference between a secure computer system and one that is vulnerable is significantly affected by the manner in which employees adhere to security policies and measures. Security awareness needs to become a part of every employee's day-to-day function in order to protect DOI's information technology and information assets. With the introduction of the personal computer, complete centralized control of computer security ended. Because of this, there is an increase in the potential for unauthorized access, modification, disclosure, and destruction of sensitive data.

Although people outside the organization (hackers, vandals, etc.) pose a threat to Government computers, a significant number of threats come from within. According to a report by the Federal Bureau of Investigation, approximately one-half of all security breaches come from within an organization. Sometimes these security breaches are malicious attacks. Many times these breaches are enabled by a lack of education or awareness on the part of a given employee. Access controls, not external threats, are the greatest obstacles in securing information and ensuring integrity.

What are your computer security responsibilities?

Computer User Responsibilities

- Protecting computer equipment and sensitive information you are authorized to access, including Privacy Act Information;
- All activity must be performed using your individually assigned User Identification (ID) and password;
- Reporting incidents involving IT security risks (e.g., password violations, virus infections, unauthorized access); and
- Being appropriately trained on the computer system(s) you access.

Supervisor's Responsibilities

- Supervisors shall ensure that their employees (both federal and nonfederal) are aware of and observe all DOI/Bureau IT security requirements and the authorized use of Government office equipment.
- Supervisors shall ensure that their employees (both federal and nonfederal) are aware of and observe all legal requirements concerning the use of proprietary software, e.g., respecting copyright and site licenses.
- Supervisors shall ensure that only authorized software runs on government computers.

IT Security Best Practices

1. IT Security Incidents

Employees are required to report all IT security incidents to their local IT Security Manager and to their supervisors. Some examples of IT security incidents are:

- Breaking into a computer and gaining control for unauthorized activities;
- Sending offensive email messages; or
- Planting malicious code such as computer viruses.

NOTE: Unauthorized access or misuse of Bureau computer systems may subject violators to criminal, civil or administrative action. Criminal penalties include fines and/or imprisonment of up to 10 years. Disciplinary action for administrative violations of the following rules may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or other action as deemed appropriate.

2. User ID & Password

You will receive a User ID (login) and initial password that is only to be used by you while working on the initial fire assignment for a specific Dispatch Center. You will be prompted to change the password when you log in for the first time. User IDs and passwords are not to be disclosed or shared with anyone including Bureau systems support personnel. If you believe your assigned User ID and password have been compromised, immediately notify your local IT Support Personnel or the local IT Security Manager. **You are responsible for all activity logged under your User ID.**

Passwords are the main defense against intruders. Users must select strong passwords and protect them carefully.

The following lists the DOI password policies. All users using DOI/Bureau computer systems **MUST** use strong passwords. Strong passwords have the following characteristics:

Password Policies:

1. Passwords will be twelve or more characters in length.
2. Passwords are required to have at least one upper case and one lower case letter.
3. There will be at least one numeric character (0, 1, 2, 3...9) in the password.
4. There will be at least one special character (e.g., %, &, #, *, etc.) in the password.
5. Passwords are to be changed at required intervals or, at a minimum, every 60 days.
6. When changing your password, at least two characters shall be unique. For example, **do not** reuse the same password and add a 1, 2, 3, etc. on the end or beginning (e.g., Secret#01, Secret#02, ...).

Again, user IDs and passwords are not to be disclosed or shared with anyone including Bureau systems support personnel. If you believe your password has been compromised, immediately change your password and notify your supervisor and the local IT Security Manager. Passwords will be changed at required intervals or any time you feel the possibility exists that it may have been compromised. Here are some basic rules when creating passwords:

- **Do not** use personal information (e.g., telephone numbers, names of family members, pets, etc.) for your passwords.
- **Do not** tape user IDs and passwords to desks, laptops, walls, or terminals, or write them down and store them in list finders, desk drawers, etc.
- **Do not** store user IDs and passwords in an unsecured computer file. This is especially important for laptop, notebook, and handheld computers since they are easy targets for theft.
- **Do** use passwords that are hard to guess but easy to remember.

An excellent method for creating a very strong password is to combine, rearrange, and jumble a two-word phrase. For example, use the two-word phrase “hot cat”. Hot cat (without the space) has 6 characters so put the number “6” in the middle of the password, then reverse the spelling and capitalize the first letter of the first word and get “Toh6tac”. If you add an * to the end of the password you get the very strong password: “Toh6tac*”, which meets all of the password rules and can be easily recreated by the person using it.

Violation of the strong password policy can result in cancellation of an account and potentially loss of future access.

3. **Computer Log off**

Either log off or use a password protected screen saver when you are away from your workstation. Password protected screen savers shall comply with the password rules listed above. Always log off when you leave your computer for the day. Password protected screen savers are not a secure substitute for logging off at the end of the workday. Remember, you are responsible for all activity logged under your User ID, and you can be held accountable for any violations that are traced to your account!

4. **Computer Viruses**

At a minimum, computer viruses can be an annoyance; at their worst, they can destroy or steal the data on your computer’s hard drive or network servers! Although the DOI uses anti-virus software, your best defense is vigilance in the form of common sense. Never use software or other executable files obtained from the Internet. These may contain hidden viruses. Scan any media (e.g., CDs, DVDs, thumb drives, etc.) that has been received from an outside source.

The most common method of distributing computer viruses today is through email and the Internet. Email virus writers need to make their messages as generic as possible to entice the greatest number of people to read them and open the attachments. Beware of anything you do not recognize or are not expecting. Typical messages are worded as:

"For your information..."
"Here is that address you requested..."
"You've got to see this..."

The best way to handle this and any similar message is to delete it. **NEVER OPEN THE ATTACHMENT!** In most cases, the message itself will not cause a problem, only the attachment.

Employees should keep in mind these simple rules:

- If the sender is someone you know but the message, and/or attachment, is unexpected or suspicious, call the person. And don't be tempted by jokes, etc, from any source. Even if you know the sender, you really don't need to see the latest animated cartoon -- not at the risk of losing valuable data, impacting technical support personnel, and causing potential embarrassment to yourself or your agency.
- Do not forward suspicious email messages to other users, including outside email addresses. If the email attachment does contain a virus, you'll help to spread it to others.

Some Internet sites may also contain viruses, and just visiting these sites can infect your computer! These viruses are commonly distributed through malicious code, small computer programs that are downloaded and executed on your computer. Malicious code can be downloaded by clicking on a link, or even running your mouse pointer across an object on the web page.

The best way to avoid viruses on malicious web pages is to avoid visiting unnecessary web sites. Limiting your browsing to web sites for conducting official business only will significantly reduce this risk!

By following these simple rules, you can help limit the spread of viruses and other malicious code.

5. Sensitive Data Storage

Sensitive information is defined as:

Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. [15 USC Sec. 278-g3].

In plain English, sensitive data is information pertaining to individual employees (SSN, home addresses, etc.), pending contract information, certain financial records and other information that if disclosed could be detrimental to an employee's privacy or the Bureau's mission. Ideally, sensitive data should not be stored on your computer's local hard drive unless it's encrypted. Sensitive data stored on removable media (diskettes, CD-ROMs, thumb drives, etc.) shall be encrypted requiring a strong password for decryption wherever possible or locked away in a local secure location (not removed from agency custody) when not in use and encryption software is not readily available.

When disposing of media containing sensitive data, the media must be physically destroyed before discarding. Erasing files is not enough! These files can be easily retrieved.

6. Authorized Software

Only authorized and licensed software may be installed. Unauthorized software may conflict and damage other software or its data, may contain malicious code or be in violation of copyright laws. It is illegal to make unauthorized copies of copyrighted software.

7. Protect Equipment

Keep food, drink and other hazards far away from your computer.

8. Protecting the Work Area

Keep unauthorized individuals away from your computer equipment and data. Always challenge strangers. Do not throw away or recycle paper documents containing sensitive data; shred them! Destroy diskettes, CD-ROMs and other media before disposal. This can be accomplished by scratching the readable side of the CD/DVD, cutting the disk with scissors or using a shredder (this is the best option where available). Floppy diskettes can be destroyed by removing the floppy diskette platter inside the diskette casing and cutting the media into several pieces with a pair of scissors or other sharp object.

9. Social Engineering

Employees can be fooled into giving out information to hackers through a technique called “social engineering”. Social engineering is a term to denote various scams used by hackers to obtain information from unsuspecting employees through deception, disguise and/or coercion. The goal of the hacker is to get you to disclose your user ID and password so they can gain access to our computer systems and networks. Typically, the technique is used over the phone or via email. Many times the hacker will pose as a computer support technician, contractor, or other authorized personnel. Here are some of the tell-tale signs that should alert you to the possibility of a social engineering attempt.

- Reluctance to provide contact information: If you say, “Can I have a number to call you back?” you might well hear a click. Some techniques a hacker may use are, “I’m on a cell phone: my battery’s dying. I’ll call you back in an hour after you gather this information for me.”
- Rushing: Is the person on the other end of the line really in a rush? They might say, “Hey, somebody’s waiting for this!” Are they pushing you too hard? Are they screaming at you? When in doubt take their name and number and raise the request to your supervisor with your concerns.
- Name-dropping: Remember, a social engineer might have a copy of your organization’s internal phone list or organizational chart.
- Intimidation: Is the caller bullying you? Has your job been threatened? They might say, “I’ve been transferred four times, let me have your name, if you don’t help me...”
- Small mistakes: Listen for misspellings, misnomers, odd questions and other blunders.

- Requesting forbidden information: If someone says they need your password, they're lying. Do not give it to them.

10. Improper Use of Government Office Equipment

All users of the Department of the Interior (DOI) computer systems shall read and consent to the following *Notice of Monitoring* prior to access being granted:

WARNING TO USERS OF THIS SYSTEM

THIS IS A NOTICE OF MONITORING OF THE DEPARTMENT OF THE INTERIOR (DOI) INFORMATION SYSTEMS. 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.

Unauthorized or improper use of Government office equipment could result in disciplinary or adverse personnel action, as described in the Department of the Interior (DOI) Personnel Handbook on Charges and Penalty Selection for Disciplinary and Adverse Actions, or loss of use or limitation on use of equipment, criminal penalties, and/or employees being held financially liable for the cost of improper use.

- a. Employees are prohibited from using government office equipment, internet access, and e-mail for personal uses except as authorized by Bureau policy.
- b. Employees are prohibited from using Government office equipment, at any time, for activities that are illegal; e. g., gambling (5 CFR 735.201), or that are inappropriate or offensive to co-workers or the public, such as the use of sexually explicit material or material or remarks that ridicule others on the basis of race, creed, religion, color, sex, disability, age, national origin or sexual orientation.
- c. Employees are prohibited from using Government office equipment at any time for any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in political activities.
- d. Employees are prohibited from using Government office equipment at any time to make purchases for personal commercial gain activity.
- e. Employees are not authorized to remove Government property from the office for personal use.

- f. Employees are prohibited from using Government-provided access to the internet to present their personal views in a way that would lead the public to interpret it as an official Government position. This includes posting to external news groups, bulletin boards, or other public forums.
- g. Employees are prohibited at any time from using the Internet as a radio or music player. Such live stream use of the Internet could strain the DOI network and significantly slow communications, inhibiting DOI employees from conducting official business.
- h. Employees are prohibited at any time from using “push” technology on the Internet or other continuous data streams, unless they are directly associated with the employee’s job. Push technology from the Internet means daily, hourly or continuous updates via the Internet; e.g., news, stock quotes, weather, and similar information. Continuous data streams could degrade the performance of the entire network.

11. Additional Information

Additional information on IT Security and acceptable use policies can be found in the local Bureau’s *Information Technology Security Policy Handbooks* and DOI’s *Policies on Limited Use of Government Equipment and Telephone Use*. Both documents are available from IT Security Managers.