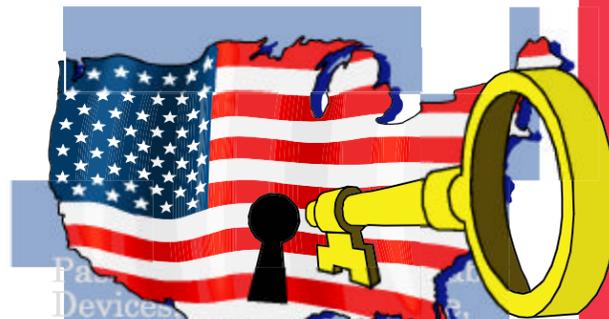


VIII. PHYSICAL SECURITY

- ✓ Retain close control of sensitive materials. Shield sensitive materials from unauthorized viewing when in use.
- ✓ Keep sensitive information in locked cabinets or drawers when not in use. Shred sensitive documents immediately after use or after their retention period has expired.
- ✓ Only personnel working with sensitive data should be allowed access to the area where sensitive data is being reviewed or discussed.
- ✓ All visitors, including family, should follow official visitors procedures. Signs should be posted to direct visitors to acceptable areas and to restrict their access to work areas.
- ✓ Visitors should meet with employees in a common area, such as a conference room, that is away from workstations and work areas which could have sensitive materials.

Security Expectations



USDA
Food Safety and Inspection Service

I. PASSWORDS

- ✓ Use alphanumeric passwords that are not easy to guess. Even include special characters, if supported by the operating system, to make it as difficult as possible for your password to be guessed by someone else.
- ✓ Words contained in dictionaries, spelling lists, and other word lists should not be used as a password. Software programs from hackers can breach easily constructed passwords, e.g. computer1.
- ✓ Do not choose a password that can be guessed or associated with you, such as your street address, license plate number, or name spelled backwards followed by a number.
- ✓ Protect your passwords from disclosure. Do not share your passwords with others. Do not post your passwords anywhere in your work area, such as under your keyboard, on the monitor, or in an unlocked desk drawer.
- ✓ Your workstation must be protected from unauthorized access whenever you leave it. Therefore, whenever you leave your workstation, you must either log off, or manually invoke your password-protected screen saver, or have set the time for automatically invoking your password-protected screen saver to ensure your unattended workstation is protected from unauthorized access.
- ✓ Change your password immediately and notify your supervisor if you believe that your password might be known by someone else or that someone has gained unauthorized access into your system.
- ✓ Do not store or embed your user login ID or password in an automatic script routine or shortcut that could potentially facilitate unauthorized access.
- ✓ Password distribution must be done securely so that only the intended recipient of the password receives the information.

II. VIRUSES

- ✓ If you suspect a virus has infected your workstation, stop using your system and immediately notify your supervisor or security office.
- ✓ Do not participate in chain letters of chat rooms, download games, files or programs, or access inappropriate or questionable Web sites since these activities increase the potential that viruses, Trojan Horse programs, or other malicious files or programs will be loaded to your workstation and network.
- ✓ To minimize the introduction of viruses, ask friends and family not to send you any e-mail messages with non-work related attachments to your government e-mail address.
- ✓ Do not open attachments in your e-mail if you are not familiar or comfortable with the extension for the attachment. Viruses may be embedded in the attachment, such as an attachment with the extension .exe. If a message does not fit the normal patterns for e-mail you receive, be cautious and do not open the attachment until you verify the validity of the attachment by contacting the sender.
- ✓ Scan diskette or CD for viruses before use.

III. EMAIL

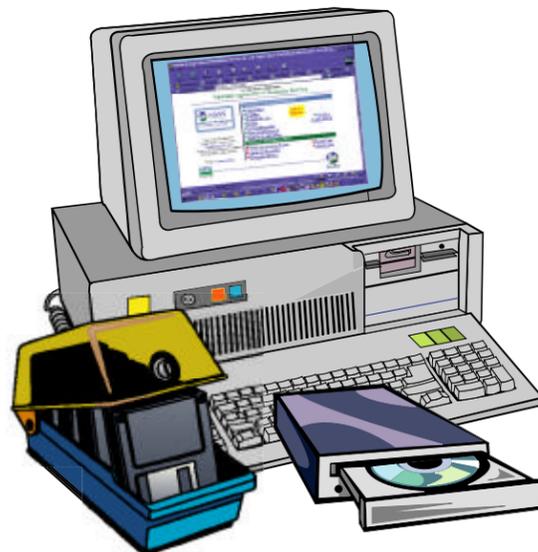
- ✓ Sending an e-mail message is like mailing a postcard – you don't know who might eventually read it, so assume everyone can.
- ✓ Address e-mail carefully. Verify you are sending the message to the correct person.
- ✓ Frequently update any e-mail distribution lists you might have created to ensure former or transferred employees are deleted from the lists.
- ✓ Verify the file name and contents of any attachment to your outgoing e-mail to ensure sensitive information is not being sent to an unauthorized individual.
- ✓ If you receive material via e-mail that is inappropriate, such as pornographic material, notify your supervisor..

IV. SENSITIVE DATA

- ✓ You are responsible for always protecting the confidentiality of sensitive data and information. Do not disclose or discuss any sensitive data or information with unauthorized individuals.
- ✓ Do not share any sensitive information on the telephone, voice mail, or e-mail.
- ✓ You should refer anyone asking questions about sensitive information to your supervisor.
- ✓ Access to sensitive data or information within USDA and FSIS must be kept to a "need to know" basis.
- ✓ When training, do not share any sensitive or confidential data or information with trainees that they do not need to know to perform their work responsibilities.
- ✓ Never store sensitive data or information on your computer's hard drive.

V. SOFTWARE

- ✓ Do not access, modify or copy any account, file, or application that is not required to perform your official duties.
- ✓ Do not install or use unauthorized software, "Peer to Peer" software, and "file sharing" products, such as Morpheus and Kazaa, on equipment used to conduct government business.
- ✓ Only grant directory rights for sensitive information to authorized personnel.
- ✓ Do not download software from the Internet to office computers, such as freeware, shareware, or public domain software, without proper approval and without scanning for potential viruses.
- ✓ Observe all software license agreements concerning issues such as distribution of software. Do not violate copyright laws. You are personally responsible for all costs or fines resulting from copyright infringement.



VI. OFFICE EQUIPMENT

- ✓ Confirm the identity of anyone repairing a computer or other equipment in your area.
- ✓ Vendors must be escorted and monitored at all times while performing maintenance duties.
- ✓ Do not move equipment into or out of your work area or exchange computer components without required authorization.
- ✓ Double check that there is no sensitive information on your computer prior to sending it out of the office for service.
- ✓ Follow policy and take appropriate steps to thoroughly clean hard drives before equipment is reassigned, surplus, or discarded.
- ✓ Do not create any unauthorized connections to other systems or services.
- ✓ Protect computer equipment from potential hazards, such as food, drink, staples, and paper clips.
- ✓ Promptly report security incidents to your supervisor, such as theft of equipment or software, or unauthorized disclosure of data or information.



VII. ALTERNATE WORK SITES

- ✓ All security measures at the workplace should also be followed while working at home or a satellite work site. For example, always protect your computer from unauthorized viewing by using a password-protected screen saver.
- ✓ Do not take copies of sensitive materials to your alternate work site.
- ✓ Never store sensitive information on the workstation at your alternate worksite.
- ✓ Remember - if you use the agency access server at any time, you are using government property.
- ✓ If supported by your workstation, you should disable the screen and keyboard at your host location when remotely accessing your computer so that someone cannot see your work at the host location.
- ✓ Do not share a telephone number or remote access procedure with an unauthorized individual or with anyone over the telephone.
- ✓ Use caution when exchanging files between your office and alternate site's workstation. These files can contain viruses, especially if a home personal computer is also used by other family members, and must be scanned before use.

