PHYSICAL SECURITY

Retain close control of sensitive materials. Shield sensitive materials, such as completed questionnaires, summary printouts, and charts with survey indications, 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 the sensitive data should be allowed access to the area where these data are being reviewed or discussed.

All visitors, including family, should enter the office through the reception area. Door signs should be posted to direct visitors to the reception area 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 have sensitive materials.

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.

AGRICULTURE COUNTS NASS

NASS

FACT FINDERS FOR AGRICULTURE

UNITED STATES DEPARTMENT OF AGRICULTURE

Security Expectations

PASSWORDS

Use alphanumeric passwords that are at least eight characters in length. 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 passwords. Hackers can breach easily constructed passwords.

Do not choose a password that can be guessed or associated with you. These include street addresses, license plate numbers, or names 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, manually invoke your password-protected screen saver, or have set the time for automatically invoking your password-protected screen saver to less than five minutes to ensure your 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.

VIRUSES

Antivirus software must be installed and active on all devices, including portable devices connected to or accessing the NASS network.

No persons shall write, distribute, or introduce any software known or suspected to be infected with viruses, worms, Trojan Horses, or other malicious code into the Agency's computing environment.

If you suspect a virus has infected your workstation, stop using your system, disconnect it from the LAN, and immediately notify your supervisor and LAN Administrator.

Do not participate in chain letters or chat rooms, download unauthorized files or programs, or access inappropriate or questionable websites since these activities increase the potential that viruses, Trojan Horses, spyware and other malware will be loaded to your workstation and the Agency's network.

To minimize the introduction of viruses and other malware, ask friends and family not to send you email messages with non-work related attachments to your government email address.

Do not open attachments in your email if you are not familiar or comfortable with the extension of the attachment (e.g. exe, vbs, zip, etc.). Viruses may be embedded in the attachment. If a message does not fit the normal patterns for email you receive, be cautious and do not open the attachment until you verify the validity of the attachment.

Any portable storage media (i.e. diskette, CD, flash drive, etc.) used on personal equipment should be scanned for viruses before being used on office equipment.

ELECTRONIC MAIL

Sending an email message is like mailing a postcard - you don't know who might eventually read it, so assume everyone can.

Address email carefully. Verify you are sending the message to the intended person.

Frequently update any email distribution lists you might have created to ensure former or transferred employees are deleted from the lists.

Verify the filename and contents of any attachment on your outgoing email to ensure information is not being sent to unauthorized individuals.

If you receive material via email that is inappropriate, such as pornographic material, delete it immediately.

A user shall not use computing and communications facilities to harass others or interfere with their work. This includes sending obscene, abusive, fraudulent, threatening, or repetitive messages to other users.

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, such as names from our list frame, survey data, survey indications, and recommendations from a Field Office.

Do not share any sensitive information via telephone, voice mail, or email.

You should refer reporters or anyone else asking questions about sensitive information to your supervisor.

Access to sensitive data or information within our Agency must be kept to a "need to know" basis.

Only grant directory rights for sensitive information to authorized personnel.

Do not share sensitive or confidential information during training or meetings if participants do not have a need to know.

Never store sensitive data or information on your computer's hard drive, or any portable storage media.

Dispose of computer media according to Agency-approved means. CD's and DVD's should be shredded using the CD/DVD shredder provided for this purpose.

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.

Unauthorized instant messaging software, such as Yahoo Messenger, AOL Messenger, and ICQ, is prohibited from being installed on Agency computers.

Do not download software from the Internet to office computers, such as freeware, shareware, or public domain software, without your supervisor's 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.

HARDWARE

Do not move equipment into or out of your work area or exchange computer components without approval from your supervisor.

Double check that there is no sensitive information on your computer prior to sending it out of the office for service.

Computer hard drives must be erased with tools approved by the Computer Security Staff before disposal.

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.

Do not tamper with any Agency-owned equipment.

Installation of unauthorized wireless networks or access points within NASS space is prohibited.

PORTABLE ELECTRONIC DEVICES

Keep portable electronic devices close at hand at all times. Do not check them as baggage or put them on luggage carts when traveling.

Do not store sensitive data or information on a portable electronic device.

If using your portable electronic device for work while in transit, be sensitive to fellow travelers looking over your shoulder.

All portable electronic devices must be password-protected.

REMOTE ACCESS

All security measures at the workplace should also be followed while working at home or at a satellite work site. For example, always protect your computer from unauthorized viewing by using a password-protected screensaver.

Do not take copies of sensitive materials to an alternate work site. This includes materials such as names and addresses from our list frame, completed questionnaires, charts with indications and estimates, and draft releases with estimates that have not been published.

Never store Agency information on the workstation at your alternate worksite.

If supported by your workstation, you should disable the monitor and keyboard at your host location when remotely accessing your computer so 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 and must be scanned before use.

Remember, if you connect to the NASS network remotely via Virtual Private Network (VPN) or other approved means, you are using government property.

Remote access users must not share tokens, passwords, or any other access devices with anyone.

Remote users must never lend to unauthorized personnel handheld computers, PDAs, smart phones, or any other computing device that stores information about business activities.