

**National Information Security Handbook**

**PART 600 - GENERAL**

600.0 Purpose

600.1 Major Laws and Guidelines Governing Security

600.2 Security Representatives

600.3 User Responsibilities

600.4 Performance Plan Elements for Security

## PART 600 - GENERAL

### 600.0 Purpose

This handbook is constructed to help IT specialists, system administrators, and end users quickly find answers to specific questions about what to do in situations concerning security. Items covered include computer operations and access, electronic mail and the Internet, safeguarding and protecting data, training, reporting procedures, security plans, and local area networks. Additional sections will be added as the need arises. This handbook is aimed at Federal employees, partners, Government contractors, and others who have access to government computers. Part 615.0 contains a list of definitions and Part 615.1 contains commonly asked questions. Relevant policy is in the National IRM Manual, which is available on-line at [www.nrcs.usda.gov](http://www.nrcs.usda.gov).

### 600.1 Major Laws and Guidelines Governing Security

- (a) [Computer Security Act of 1987, Public Law 100-235](#). This law requires Federal agencies to identify computer systems that process sensitive information, prepare and maintain computer security plans for sensitive systems, and conduct computer security training for employees involved in the operation or use of sensitive systems.
- (b) [Freedom of Information Act \(FOIA\) of 1980, Public Law 93-502](#).
- (c) [Paperwork Reduction Act](#), revised 1986. This provides for the administration and management of computer resources.
- (d) Implementation of Gateway and Firewall Policy and Technical Security Standards, DN 3140-6.
- (e) Implementation of Securing Sensitive Information on Servers, DN 3140-8.
- (f) Network Protocol Analyzers, Departmental Note (DN) 3140-9.
- (g) [Security Requirements for Government Employees, Executive Order Number 10450, April 1953](#).
- (h) [Security of Federal Automated Information Systems, Appendix III, Office of Management and Budget \(OMB\) Circular Number A-130, February 1996](#). This directive stipulates that each agency shall implement a comprehensive automated information systems security program. The appendix establishes the basic managerial and procedural controls that must be included in Federal automated information systems.
- (i) [USDA Automated Data Processing \(ADP\) Security Manual, Departmental Manual \(DM\) Number 3140-1, July 1984](#). This document contains standards, guidelines

and procedures for the development and administration of IT security programs mandated by DR 3140-1.

(j) [USDA Information Systems Security Policy, May 1996](#), Departmental Regulation (DR) 3140-1.

(k) [USDA Internet Security Policy, March 1995](#), DR 3140-2.

(l) Government Information Security Reform Act of 2000, Public Law 106-398. This Act requires an agency to develop and implement an information program and to provide information security for the operations and assets of the agency.

(m) [Telecommunications and Internet Services and Use, USDA DR 3300-001, March 1999](#). Authorizes the limited personal use of telecommunications resources by USDA employees in the workplace on an occasional basis with prior supervisory approval provided use occurs during the employees non-work time, involves minimal expense to the government, and does not interfere with official business.

(n) [Presidential Decision Directive 63: Critical infrastructure Protection, May 1998](#). This directive requires that the United States take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems.

(o) Computer Fraud and Abuse Act of 1986. This law provides for punishment of individuals who access Federal computer resources without authorization, attempt to exceed access privileges, abuse Government resources, and/or conduct fraud on Government computers.

A complete list of policy documents that relate to security may be found in the National IRM Manual, Part 502.

## 600.2 Security Representatives

Each NRCS office manager is responsible for security within that office. The NRCS office manager may delegate these duties to a local security representative. There shall be at least one security representative designated for each physical office location. This person shall coordinate information security issues with the State IT specialist or designated security officer. Part 615.2 is a listing of NRCS Security Officers.

The roles and responsibilities for the Chief Information Officer, National Security Officer, and Deputy Security Officers are detailed in the National IRM Manual, Part 502.

Security roles and responsibilities for Common Computing Environment (CCE) equipment system administrators are defined in CCE documentation.

### 600.3 User Responsibilities

NRCS computer users are responsible for the following:

- (a) Complying with USDA, NRCS, and Information Technology Working Group (ITWG) security policies and regulations.
- (b) Accessing the USDA network with a unique user name (at least seven characters) and password.
- (c) Ensuring that passwords are not the same as your user ID.
- (d) Changing network and workstation passwords as required. Users must also change passwords when it is suspected that someone has tried to use their user ID or password to gain access to an NRCS computer.
- (p) Changing their network and workstation password the same day they receive their user ID and initial password.
- (p) Not writing down passwords or storing them in unsecure locations.
- (p) Not sharing passwords with anyone.
- (p) Not storing passwords on discs, diskettes, tapes, CD-ROMs, or in scripts.
- (p) Periodically backing up data files on the hard disk onto backup media (diskettes, tapes, CD-ROM, etc.).
- (p) Not deliberately circumventing security features of the operating system on workstations or network servers.
- (p) Not leaving workstations logged on to the local area network or a World Wide Web site.
- (p) Storing laptops and other portable equipment in a secure location at the end of the day. This does not include car trunks or truck storage boxes.
- (p) Not installing any software that has not been approved by NRCS management and the Interoperability Lab (IOL).
- (p) Using Government computers for official duties and not for personal gain.
- (p) Providing access to sensitive data only to individuals who have an established need to know.
- (p) Not using a local area network server or Web server as a workstation.

(q) Disclosing only information that would be provided under the Freedom of Information Act.

#### **600.4 Performance Plan Elements for Security**

(a) A security element must be included in each IT manager's and IT employee's Performance Work Plan (SCA Form 440). A sample element is provided below:

Complies with USDA and federal security laws, regulations, and policies. Ensures security training is on their Individual Development Plan and the plans for all subordinate IT staff members. Ensures that all supervised employees receive and are credited with completion of agency-provided security awareness training. Enables employees to become familiar with security practices and policies based on their responsibilities. Incorporates security measures and practices in assigned duties.

(b) A security element may be included in other employee's Performance Work Plan. A sample below is provided below:

Complies with USDA and Federal security laws, regulations and policies. Attends scheduled agency-provided security awareness training. Incorporates security measures and practices into assigned project activities.

**PART 601 – COMPUTER OPERATIONS**

**SUBPART A – PHYSICAL SECURITY**

601.0 General

601.1 Physical Security

**SUBPART B - COMPUTER ACCESS**

601.10 General.

601.11 Passwords

**SUBPART C - SOFTWARE SECURITY**

601.20 Software license agreements

601.22 Software backups and serial numbers

601.23 Modifications

601.24 Storage Media

601.25 System Backup

## **PART 601 – COMPUTER OPERATIONS**

### **SUBPART A – PHYSICAL SECURITY**

#### **601.0 General**

Computer equipment is an essential part of NRCS operations and must be protected.

#### **601.1 Physical Security**

Physical security, an integral part of protecting data, is vital in a balanced security program. Physical security involves protecting offices containing computers and related equipment from environmental threats such as fire, flood, windstorm, physical threats to people, and equipment and environmental contamination.

a. **Shared responsibility.** Responsibility for each piece of equipment is shared jointly among the head of each office, the designated security representative, the Information Resource Manager (IRM), the system administrator, and the individual(s) using that equipment in a decentralized environment.

b. **Minimum protection standards.** For purposes of this Security Handbook, the following standards have been developed as the minimum that must be followed. However, stricter standards for any given site or office may be developed and are encouraged.

(1) **Locked rooms.** Servers shall be in a locked room or a locked cabinet that is not visible from open areas.

(2) **Sensitive data.** Store sensitive data in locked or secured area. Sensitive data must not be visible on a monitor or left unattended on a printer or a desk.

(3) **Placement.** Equipment and/or data shall not be placed in an area easily accessible that would enable quick entrance and egress.

(4) **Positioning.** Computer screens or printers shall be positioned such that casual passersby shall not have access to the data. Monitors with sensitive information visible should not be left unattended. Institute a timeout so that after a minimum of fifteen (15) minutes of inactivity, the screen saver will come on and lock the workstation with a password. Alternatively, lock the workstation by simultaneously pressing the Ctrl-Alt-Delete and selecting “lock workstation.” This will secure the unattended workstation.

(5) **Eating/drinking.** Eating and drinking are prohibited in the immediate vicinity of any computer equipment. Spilled liquids and food particles on a keyboard can cause a malfunction. On magnetic media, spills can cause irreparable damage.

## National Information Security Handbook

(6) Smoking. All Federal facilities have been designated as smoke-free environments for Federal employees, partners, contractors, and members of the public visiting or using Federal facilities pursuant to Executive Order 13058.

(7) Basic safeguards. Equipment and storage media shall be protected from electrical current fluctuations, temperature, humidity, and air pollution. These basic protections shall include surge protectors, temperature control (air conditioning) and filters where appropriate.

(8) Fire protection.

(a) Fire extinguisher. An inert gas-type fire extinguisher shall be placed in the immediate vicinity of the equipment. Employees, partners, and contractors shall be trained on the proper operation of the fire extinguisher. Contact the local fire department to ascertain if they will provide training on fire extinguisher use and maintenance.

(b) Smoke detectors. Smoke detection devices shall be used to minimize the damage that may be caused by fire. All agency offices shall comply with the General Services Administration, zoning, or local fire department regulations.

(9) Cleaning. Agency employees, partners, and contractors should be cautious in making sensitive data available. Names of the custodial personnel shall be retained for audit purposes or in the event of missing equipment.

(10) Access controls. Access controls shall be in accordance with building requirements.

(11) Maintenance. Maintenance and repair personnel shall have access based upon building requirements.

(12) Reporting incidents. Any theft, damage, or illegal access to the premises and/or equipment, no matter how minor it might appear, shall be reported to the employee's supervisor who will notify the State security officer. The State security officer will notify the National Security Officer.

(13) Equipment accountability. All computer equipment is tracked in the CCE Equipment Acquisition Tracking System (EATS) database located on a server in Fort Collins, Colorado. All installations and relocations must be recorded in EATS.

(14) Collocation. Where agency offices are collocated with other Department offices, each agency shall cooperate in protecting the computer resources, data, and personnel.

**PART 601 – COMPUTER OPERATIONS**

**SUBPART B - COMPUTER ACCESS**

**601.10 General.**

All levels of NRCS deal with sensitive information. The information may be subject to the Privacy Act; it may be procurement sensitive; it may be business sensitive. Protect paper information from prying eyes and protect the information when it resides on a computer. The following precautions will minimize unauthorized access to NRCS equipment.

- (a) Restrict access to NRCS computer rooms and equipment to authorized users only.
- (b) Equipment in public areas should be placed in a way that minimizes the risk of unauthorized access. The screen of a workstation should be placed so that a customer cannot see the screen without permission.
- (c) A workstation must be operational when unattended. If a workstation must be left unattended, either shut down the system or protect it with a password.

**601.11 Passwords**

The first line of defense against illegal computer access is a good password. The objective when choosing a password is to make it as difficult as possible to gain illegal entry. Table 1 outlines some basic strategies for choosing a password.

Table 1 – Password Strategies

	<b>Recommended</b>	<b>Your Site</b>
Does your password contain your first or last name, spouse or children’s name?	NO	
Does your password contain all digits or all the same letter?	NO	
Does your password contain words contained in dictionaries?	NO	
Are strong passwords used – at least eight (8) characters including at least three of the following: lower case, upper case, numbers, and special characters.	YES	

National Information Security Handbook

Have you shared your password with others?	NO	
Have you written your password down and left it in your work area or other unsecured place?	NO	
Does your system prompt you to change your password?	YES	
Do you use the "remember password" feature?	NO	
Are login ID's kept secure?	YES	
Are users required to change passwords every 90 days?	YES	

## **PART 601 – COMPUTER OPERATIONS**

### **SUBPART C - SOFTWARE SECURITY**

#### **601.20 Software license agreements**

- (a) Copyright. Commercial and shareware software are copyrighted. Willful violation of the Copyright Law of the United States may result in the assessment of civil penalties of up to \$50,000 in addition to penalties associated with actual damages. Also, criminal penalties up to one-year imprisonment and/or a \$10,000 fine may be enforced. Penalties for violation of copyright laws will be paid by the employee, not by the agency.
- (b) Backup copies. Users shall conform to the software license agreement for each set of software. Some software vending companies restrict installation of their software to only one computer and allow making copies of the software for backup purposes only. Other vendors allow backup copies to be used on other machines as long as the software is not being used simultaneously on more than one machine.

#### **601.21 Commercial-off-the-shelf (COTS) software**

- (a) Approval. Prior to procurement, always obtain the proper technical authority from the Information Technology Center (ITC). The Inter-Operability Lab (IOL) Beltsville, Maryland; Farm Service Agency (FSA), Kansas City, Missouri; Natural Resources Conservation Service (NRCS) ITC, Ft. Collins, Colorado; and Rural Development, Rosslyn, Virginia, are currently working together to approve and certify commercial-off-the-shelf (COTS) software to be installed on the Common Computing Environment (CCE) platforms. Any system failure or problem that occurs as a result of installing non-certified DOS, or non-logo (Microsoft certification logo indicating it is certified for the NT environment on a CCE PC) will be the responsibility of the person who installed the non-certified software without the support of the Help Desk.
- (b) Protection. All USDA employees, partners, and contractors will protect Government interests as they perform their duties, which includes ensuring that commercial software acquired by the Government is used only in accordance with licensing agreements. Likewise, they are to ensure that any proprietary software is properly licensed before being installed on USDA equipment. This guidance does not apply to software developed by or for a Federal agency. No restrictions apply to its use or distribution within the Federal Government.
  - (1) Federal Law Guidance. Title 17, United States Code, Section 106 gives copyright owners exclusive rights to reproduce and distribute their material, and Section 504 states that copyright violators can be held liable for damages to the copyright owner. Title 18, United States Code provides felony penalties for software copyright infringement.

(2) Copyright Protections. Supervisors will ensure that the following requirements are made known to all employees, partners, and contractors, and will be held accountable for conducting periodic audits to ensure that these policies are being followed:

- (a) Install only commercial software, including shareware, that has been purchased through the Government procurement process on USDA systems.
- (b) Follow all provisions of the license agreements issued with the software and register organizational ownership. It is illegal to install any COTS product that does not have a legal license.
- (c) Do not make any illegal copies of copyrighted software. Normally the license will allow a single copy to be made for archival purposes. If the license is for multiple users, do not exceed the authorized number of copies.
- (d) Store software, licenses, manuals and procurement documentation in a secure location (e.g., a closed file cabinet).
- (e) When upgrades to software are purchased, the old version must be disposed of in accordance with the licensing agreement to avoid a potential violation. Upgraded software is considered a continuation of the original license, not an additional license.
- (f) Delete all illegal copies of software immediately.

### **601.22 Software backups and serial numbers**

Backups of commercial software shall be made only in accordance with the license agreement. Serial numbers of all software shall be recorded and stored offsite. In the event of damage to the original software, the serial number can be used to obtain a license copy of the damaged software from the vendor. Copies of any software license agreements shall be stored with the list of serial numbers.

### **601.23 Modifications**

No modifications may be made to CCE authorized/certified software installed on agency computers without the prior consent of the IOL. Changing computer program parameters, such as margins in a word processing package, is not considered to be a software modification.

### **601.24 Storage Media**

Externally supplied diskettes or other storage media shall not be used on agency computer systems unless the diskettes have first been scanned for viruses and contain a decal or label

indicating that no viruses were found. Diskettes moving among various computers is one way of transferring a virus to other systems. Although a diskette may have a decal or label, if the diskette is moved from one computer to another, the diskette shall be scanned before being used on the next computer.

### **601.25 System Backup**

Weekly computer system backup tapes shall be appropriately labeled for future identification and stored in a secure offsite location (in a locked, fireproof container in a locked room) to prevent unauthorized access to the data contained on them. Incremental backups shall be stored in a secure onsite location (in a locked, fireproof container in a locked room). On a monthly basis, test backups to ensure that all data is captured correctly. Backup procedures are in the CCE System Administrators Guide.

**PART 602 - INTERNET USAGE AND E-MAIL GUIDELINES**

- 602.0 General
- 602.1 Official Business Usage
- 602.2 Limited Personal Use
- 602.3 General Internet and E-Mail Usage Summary
- 602.4 Privacy Expectations.
- 602.5 Inappropriate Usage
- 602.6 Proper Representation.
- 602.7 U.S. National Guard and Reserve Duties, and Training Funded by NRCS
- 602.8 Record Keeping Requirements
- 602.9 Union Usage
- 602.10 Classified Data
- 602.11 Sensitive Data
- 602.12 Proprietary Data
- 602.13 Copyright Protection
- 602.14 Downloading Software
- 602.15 Uploading Software and or Data
- 602.16 Using Approved Gateways
- 602.17 Waiver Requirements
- 602.18 Compliance

## **PART 602 - INTERNET USAGE AND E-MAIL GUIDELINES**

### **602.0 General**

This part clarifies the USDA and NRCS policy for Internet and e-mail usage and lists the “do’s” and “don’ts” for employees, partners, and contractors while performing their daily assignments. In addition, reference materials and USDA policy documents are quoted and identified for further research and clarification if required.

### **602.1 Official Business Usage**

The use of the Internet is an integral part of service delivery for NRCS. USDA Departmental Regulation (DR) 3300-1, Appendix I, “Internet,” states, “USDA authorizes the use of the Internet to support Department and agency missions. Access to the Internet is provided through the USDA Internet Access Network. USDA mission areas and staff offices may utilize the Internet to support departmental and mission area responsibilities.” The Internet is a powerful tool, and its use is highly encouraged. However, some basic guidelines must be followed to ensure the protection of NRCS information assets.

The Internet may be used for, but is not limited to, the following purposes:

- (a) The communication and exchange of data between State and local governments, private sector organizations, and educational and research institutions, both in the United States and abroad.
- (b) The development of Internet Web-based projects.
- (c) The balance of interactive sharing of information without compromising USDA secured data.
- (d) The exchange of any nonsensitive data between USDA entities in support of Departmental mission, agency missions, or other official purposes. Uses may include e-mail and applications enabled by e-mail.
- (e) For the distribution and collection of information related to official program delivery and in compliance with Federal and Departmental guidelines.

### **602.2 Limited Personal Use**

USDA DR 3300-1, Appendix I, also states authorized purposes may include limited personal use, with supervisory approval, if it is determined that such communications:

- (a) Do not adversely affect the performance of official duties by USDA or the USDA employee’s organization;

- (b) Are of reasonable duration and frequency, and whenever possible, made during the USDA employee's personal time, such as after duty hours or lunch periods;
- (c) Serve a legitimate public interest (such as educating the USDA employee on the use of the telecommunications system, enhancing the professional skills of the USDA employee, job searching in response to Federal Government downsizing);
- (d) Do not put Federal Government telecommunications systems to uses that would reflect adversely on USDA or the agency (such as uses involving pornography; playing on-line games; private business; chain letters; unofficial advertising, soliciting, or selling except on authorized bulletin boards established for such use; violations of statute or regulation; inappropriately handled sensitive information; gambling; hate-oriented sites; and other uses that are incompatible with public service);
- (e) Do not overburden the telecommunications system (such as may be the case with broadcasts and group mailings) and create no significant additional cost to USDA or to the agency; and
- (f) Follow the policy of the USDA Internet Activities Board (IAB) as stated in RFC 1087, "Ethics and the Internet." This policy prohibits any activity that purposely:
  - (1) Seeks to gain unauthorized access to the resources of the Internet.
  - (2) Disrupts the intended use of the Internet.
  - (3) Wastes resources; such as people, capacity, and computer through these actions.
  - (4) Destroys the integrity of computer-based information.
  - (5) Compromises the privacy of users.

USDA DR 3300-1 states that the use of telecommunications equipment and services, such as telephones, facsimile machines, electronic messaging, computer equipment, and the Internet by all USDA employees, partners, and contractors shall be according to the requirements of 5 CFR Part 2635, Subpart G, Sections 704 and 705, and the United States Office of Government Ethics document, "Standards of Ethical Conduct for Employees of the Executive Branch."

### **602.3 General Internet and E-Mail Usage Summary**

This section summarizes the Internet and e-mail policy documents and notices released by NRCS and USDA and tries to explain them in non-technical terms to assist employees, partners, and contractors.

Federal Government office equipment and systems, including the Internet and e-mail systems, "**shall be for official use and authorized purposes.**" Government employees, partners, and contractors must follow all appropriate Federal laws and regulations, including

the NRCS National IRM Manual, USDA policies, rules of conduct, and ethics while using the Internet.

The NRCS National IRM Manual follows USDA DR 3300-1 in that it **authorizes** with supervisory approval the **limited personal use** of the Internet and e-mail “in the workplace on an occasional basis provided that the use involves minimal expense to the government and does not interfere with official business. Occasional personal use of telecommunications resources shall take place during the employees’ personal time. This guideline also follows the Chief Information Officer (CIO) Council’s model for guidance on limited personal use.” Employees will certify in writing that they understand their limitations under DR 3300-1 prior to being authorized limited personal use. Distribution lists shall be updated and kept as current as possible. Contractors shall be deleted from the e-mail directory when their contract has expired.

All employees, partners, and contractors should understand that telecommunications resources and official time shall not be used to earn outside income, nor should employees, partners, or contractors use telecommunications resources or official time for private gain. Employees, partners, and contractors shall not record overtime, compensatory time, or credit hours earned during any period of time they are using the Internet or e-mail services for personal use.

Employees, partners, and contractors shall exercise common sense and good judgment in the personal use of telecommunications resources. Official Government business always takes precedence over the personal use of telecommunications resources. While the occasional use of telecommunications resources in moderation is acceptable, uses not conforming with this policy are strictly prohibited.

Employees, partners, and contractors are expected to conduct themselves professionally in the workplace and to refrain from using telecommunications resources for activities that are inappropriate or offensive to coworkers or the public. Such activities include accessing, storing and distributing sexually explicit materials or making remarks that ridicule others on the basis of race, creed, religion, color, sex, handicap, national origin, or sexual orientation.

#### **602.4 Privacy Expectations.**

USDA DR 3300-1 states that employees and contractors do not have a right, nor should they have an expectation, of privacy while using any Government office equipment at any time, including time spent accessing the Internet and e-mail systems.

What does the prior statement really mean? To the extent that employees wish that their private activities to remain private, they should avoid using agency or Department office equipment such as their computer, the Internet, or e-mail. By using Government office equipment, employees, partners, and contractors imply their consent to disclosing the contents of any files or information maintained or passed through Government equipment.

By using government equipment, consent to monitoring and recording is implied with or without cause. This monitoring and recording includes, but is not limited to, Internet and

e-mail systems. Any use of Government communications resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

System managers can employ monitoring tools to detect improper use subject to the guidance in the National IRM Manual. Electronic communications may be disclosed within an agency or department to employees who have a need to know in the performance of their duties.

## 602.5 Inappropriate Usage

Employees, partners, and contractors are expected to conduct themselves professionally in the workplace and to refrain from using Government office equipment, the Internet, and e-mail systems for activities that are inappropriate. Misuse or inappropriate personal use includes, but is not limited to:

- (a) Any personal use that could cause congestion, delay, or disruption of service to any Government system or equipment. Examples:
  - (1) Greeting cards, videos, sounds, or other large file attachments can degrade the performance of the entire network.
  - (2) “Push” technology on the Internet and other continuous data streams (e.g., radio broadcasts, and ticker tape banners such as stock quotes, weather) would also degrade the performance of the entire network and be an inappropriate use.
- (b) Using the Government systems as a staging ground or platform to gain unauthorized access to other systems.
- (c) Creating, copying, transmitting, or retransmitting chain letters or other unauthorized mass mailings regardless of the subject matter. **Note:** This includes the transmission of chain e-mail messages, which are messages that ask each recipient to send copies to other users.
- (d) Activities that are illegal, inappropriate, or offensive to fellow employees, partners, contractors or the public. **Note:** These activities include, but are not limited to, hate speeches or materials that deride others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
- (e) Creating, downloading, viewing, storing, copying, or transmitting sexually explicit or sexually oriented materials.
- (f) Creating, downloading, viewing, storing, copying, or transmitting materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities otherwise prohibited.
- (g) Use for commercial purposes, in support of “for-profit” activities, or in support of other outside employment or business activity; e.g., consulting for pay, sale, or administration of business transactions, and sale of goods or services.

- (h) Engaging in any outside fundraising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.
- (i) Use for posting agency information to external newsgroups, bulletin boards, or other public forums without authority. Note: This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee, unless appropriate agency approval has been obtained. Otherwise, use is at odds with the agency's mission or positions.
- (j) Any use that could generate more than minimal additional expense to the Government.
- (k) The unauthorized acquisition, use, reproduction, transmission, and distribution of computer software or other material protected by national or international copyright laws, trade marks, or other intellectual property rights.
- (l) Playing on-line games.
- (m) Representing oneself as someone else.
- (n) Soliciting Government employees or providing information about or lists of USDA employees to others outside the Government without authorization.
- (o) When it interferes with the employee's job, the jobs of other employees, or the operation of the Internet gateways.
- (p) Any type of personal solicitation.
- (q) Modifying Government office equipment for non-Government purposes, including loading personal software or making configuration changes.

## **602.6 Proper Representation.**

It is the responsibility of employees, partners, and contractors to ensure that they are not giving the false impression that they are acting in an official capacity when they are using Government office equipment for non-Government purposes. If there is expectation that such a personal use could be interpreted to represent an agency, then an adequate disclaimer must be used. One acceptable disclaimer is, "The contents of this message are mine personally and do not reflect any position of the Government or my agency."

The Standards of Conduct states, "an employee shall not use or permit the use of his government position or title or any authority associated with his public office in a manner that could reasonably be construed to imply that his agency or the Government sanctions or endorses his personal activities." (5 CFR 2635.702)

## 602.7 U.S. National Guard and Reserve Duties, and Training Funded by NRCS

Employees may use NRCS information resources, including the Internet and e-mail systems, to support their U.S. National Guard and U.S. Military Reserve duties and to prepare assignments required to successfully complete NRCS-funded training as long as those activities are:

- (a) Official to the U.S. National Guard or Reserve or NRCS-funded training.
- (b) Not in conflict with NRCS duties.
- (c) Not in violation of Federal laws or USDA and NRCS policies.
- (d) Known by the employee's immediate supervisor.

## 602.8 Record Keeping Requirements

USDA DR 3300-1, Appendix F, states the following:

“Official business conducted over electronic mail systems shall comply with “Electronic mail messages that meet the definition of a record as stated in the FRA shall be preserved, for the appropriate period of time. For example, e-mail messages that document agency policies, programs, decisions, operations and functions are considered Federal Records and shall be archived.”

**Note:** NRCS backup and archive systems cannot distinguish between personal and official e-mail; therefore, backup systems will back up personal e-mail messages the same as official business e-mail messages. As a result, if and when an e-mail system is backed up, either manually or automatically, personal e-mail messages then existing on the system will be backed up as well. Consult the local system or e-mail manager if further information is needed on how frequently backups are done or how long the backups are kept, since these details differ from system to system and from site to site.

## 602.9 Union Usage

If authorized by a negotiated agreement, unions can use Government equipment and facilities in their official capacity.

## 602.10 Classified Data

The Internet and e-mail systems are not secure and **shall not** be used to transmit classified (Top Secret, Secret, and Confidential) national security material.

### 602.11 Sensitive Data

Information exempted from disclosure under FOIA (Public Law 93-502) and information protected by the Privacy Act (Public Law 93-579) **shall not** be transmitted over the Internet and e-mail systems unless encrypted. Other sensitive information **shall not** be sent unencrypted over an unprotected (uncertified or unaccredited) e-mail system.

### 602.12 Proprietary Data

Commercial proprietary information shall be protected and preserved according to the conditions under which it is purchased, provided, and used.

### 602.13 Copyright Protection

All users must obey all copyright and licensing laws. Users must also comply with [Executive Order 13103, Computer Software Piracy](#), which was issued on September 30, 1998.

### 602.14 Downloading Software

Software **will not** be downloaded if the following occurs:

- (a) There is a condition of downloading that commits NRCS to purchase the software or incur unauthorized expenses.
- (b) It exceeds the limits of NRCS software license agreements.
- (c) If it is not an approved software for the CCE computer environment.

### 602.15 Uploading Software and or Data

No NRCS software, data files, or sensitive information will be uploaded to e-mail systems and the Internet without proper authorization. This will ensure that:

- (a) No copyright-protected software is distributed through external media or systems in violation of copyright laws.
- (b) NRCS software, data, and information are distributed only to authorized recipients.
- (c) Only correct, accurate, and official versions are released.
- (d) No sensitive data or information is released.
- (e) Uploading functions are for approved official Government business only.

## 602.16 Using Approved Gateways

NRCS operating policy requires that any access to Internet and e-mail system services be provided only through USDA- and NRCS-approved gateways. Private Internet Service Providers are prohibited.

## 602.17 Waiver Requirements

NRCS offices **shall not** contract separately with a non-USDA Internet Service Provider until an Internet access technical waiver has been requested from ITC, and ITC has submitted the waiver to and has had it approved by the Department's Office of the Chief Information Officer.

## 602.18 Compliance

Any questions regarding authorized or official use of equipment in an office should be directed to the employee's supervisor, who may contact the State Security Officer for answers. Using good judgment while complying with these guidelines and policies can prevent computer security problems and assure protection of agency data.

Any person who willfully or knowingly violates or fails to comply with the provisions of appropriate Federal laws or USDA and NRCS regulations will be subject to appropriate disciplinary actions, including counseling sessions, suspension, or dismissal.

All employees, partners, and contractors shall notify their immediate supervisor, management officials, and their local Security Officer if they suspect a computer security incident or violation. The identity of the person reporting a computer security incident or violation shall be kept confidential. The identity of the person reporting the incident or violation and the information reported shall be released only on a need-to-know basis. The immediate supervisor, management officials, and local Security Officer shall notify the State Security Officer, who will follow proper reporting procedures.

Authorized personnel, such as contracting officers, information systems security officials, and LAN administrators and supervisors, may take possession of any NRCS-owned information resources or unauthorized resources at the instructions of the appropriate management official or legal authority to examine the contents for violations of Federal laws or USDA and NRCS policies.

**PART 603 - SAFEGUARDING AND PROTECTING EQUIPMENT AND DATA**

603.0 Purpose

603.1 Safeguarding Data

603.2 Safeguarding Equipment

603.3 Backup and Recovery

603.4 Computer Virus

603.5 Fax and Printed Information

## **PART 603 - SAFEGUARDING AND PROTECTING EQUIPMENT AND DATA**

### **603.0 Purpose**

This part details ways users can protect data from theft or destruction. Data is commonly stored on desktops, laptops, or servers. However, data can also be stored in cell phones or personal data accessories (PDAs).

### **603.1 Safeguarding Data**

The following are good habits users must institute to safeguard and protect data:

- (a) Maintain physical possession of the equipment (laptops, cell phones, PDAs) which will stop people from gaining access to the data.
- (b) Have password on the equipment to keep unauthorized personnel out.
- (c) Have a backup of the data in case of accidental deletion.
- (d) Have a password on screen savers. Also institute a “timeout” so that after a minimum of fifteen (15) minutes of inactivity, the screen saver will come on and lock the workstation with a password. Alternatively, lock the workstation by simultaneously pressing the Ctrl-Alt-Delete and selecting “lock workstation” to secure the unattended workstation.
- (e) Label diskettes, CD-ROM, and zip diskettes with adequate information to identify it for later use.
- (f) When the user has finished with the information, delete it from the diskette, CD-ROM, zip diskette, or hard drive.
- (g) When sensitive information is no longer needed, ensure that the diskette, tape, CD-ROM, or zip diskette is destroyed.
- (h) Protect keyboards and screens from view by the general public and others to safeguard password entries and data.
- (i) Encrypt sensitive data on desktops, laptops, and servers. One or more files can be stored in a WINZIP file; thereafter add password to encrypt the .ZIP file.

### **603.2 Safeguarding Equipment**

Laptops, cell phones, PDAs, and other portable equipment must be carried on the airplane. Do not check these items with your luggage.

### 603.3 Backup and Recovery

- (a) How often a backup needs to be performed varies according to need.
  - (1) Common Computing Environment (CCE) servers must have a backup performed as outlined in the CCE System Administrators Guide.
  - (2) CCE desktops must have a backup performed as outlined in the CCE Users Guide.
  - (3) Backups can be accomplished by putting the files on a server or backing up the data onto a tape or CD-ROM.
  - (4) Test backups to ensure that all necessary data has been captured.
  - (5) Label all backup media with appropriate information to determine the date it was done and the type of backup performed.
- (b) Offsite Storage
  - (1) Offsite storage locations may include, but are not limited to, another agency or government site, a safe deposit box at a local bank, or a commercial offsite storage facility with controlled access. An employee's home should not be considered as an alternative except emergencies.
  - (2) Offsite storage must be kept for a minimum of one month. Storage media may be recycled at the end of the three months.
  - (3) Consider storing CRITICAL data backups in another geographical location to insure that a natural disaster does not destroy your backups.

### 603.4 Computer Virus

- (a) Automated virus data update. The Information Technology Center (ITC), Fort Collins, Colorado, has instituted a procedure for capturing and distributing McAfee virus updates. These updates are transmitted to State and regional offices on a regular schedule; the State Offices then forward the updates to Service Centers.
- (b) Here are some basic steps to take that will help ensure that viruses are not downloaded to your system:
  - (1) Do not open/download e-mail or Internet files with .exe, .vbs., .bat, .com, .pif, .shs, .reg, .vbe, .wsh, .wsf, .scr, .lnk, .jse, jsf file extensions.
  - (2) Do not download e-mail or Internet files to hard disk. Instead, download to a diskette then scan the diskette for viruses.

- (3) When getting a diskette from someone else, perform a virus scan on it prior to using it.
  - (4) Do not reboot with a diskette in the PC.
- (c) If a virus is detected:
- (1) Do not turn off the machine.
  - (2) Disconnect from the network.
  - (3) Write down where you believe the virus may have originated (files, disks, e-mail, etc), who sent you the infected media, how it was sent, and the symptoms.
  - (4) Notify your security officer of the infection, how many machines are infected, and by what viruses.
  - (5) Address any remaining questions on computer viruses to the appropriate help desk.
  - (6) Have the appropriate IT person/system administrator clean the infected machine after all appropriate information is documented.
- (d) Full disk scans must be performed as directed.

### **603.5 Fax and Printed Information**

- (a) Printed material (whether sensitive or not) should be picked up from the local or networked printer right away.
- (b) Sensitive information:
  - (1) If sensitive information is to be faxed, first call the fax destination to ensure that an authorized person will be available to pick up the fax right away.
  - (2) Secure any sensitive information before leaving the office to ensure that no unauthorized personnel have access to this information.
- (c) Ensure that printed or faxed material is appropriately destroyed when it is no longer needed (i.e., sensitive information should be shredded, other information can be re-cycled).

**PART 604 - SECURITY TRAINING**

604.0 Security Awareness Training

604.1 System Administrator Training

604.2 Security Personnel Training

## **PART 604 - SECURITY TRAINING**

### **604.0 Security Awareness Training**

The Computer Security Act of 1987 requires that Security Awareness Training be held annually. The following individuals are required to participate in the training: all NRCS employees, all NRCS volunteers using NRCS computer systems, district and other partners, individuals not affiliated with NRCS who have authorization to use NRCS computer systems, and contractors officially located where NRCS computers reside.

The NRCS Security Awareness Training will provide participants with practical information on computer security, which must be immediately implemented in their daily duties. The following topics must be included in this training: policy, responsibility, and accountability; threats and vulnerabilities; passwords; and data/software communications; physical security; and FTS security information.

“Computer Security Awareness,” a course developed by the National Employee Development Center and the NRCS security team, is the required training course for Security Awareness Training in NRCS. The course is designed for use in a facilitated training session or as an individual study guide. Course materials will be distributed to training officers at National Headquarters and State and regional offices. To receive additional copies of course materials, contact your training officer.

Individuals (Government employees, contractors, and district employees) will certify completion of the Security Awareness Training by completing the memo in Part 615.3.

State security officers will send certification to the National Security Officer that all employees, partners, and contractors have completed the security awareness training. A copy of this certification will also be sent to State training officers and regional IT specialists.

### **604.1 System Administrator Training**

The deployment of CCE equipment will include training on how security is handled in Win 2000 Operating System.

### **604.2 Security Personnel Training**

In addition to the annual security awareness training, State and regional security personnel need to keep current on changes in the security field. The following are Web sites that will provide security personnel with valuable information on training sessions and conferences. It is recommended that at least one additional training session on security be attended each year.

<http://www.sans.org/giactc/courses.htm>

## National Information Security Handbook

<http://howto.lycos.com/lycos/cl/0,,14,00.html>

<http://www.misti.com/>

[http://csrc.nist.gov/ATE/training\\_&\\_education.html](http://csrc.nist.gov/ATE/training_&_education.html)

<http://www.nsa.gov/isso/>

<http://www.verisign.com/training/index.html>

<http://www.learningtree.com>

**PART 605 - REPORTING PROCEDURES**

605.0 General

605.1 Entrance and Exit Conference

605.2 Theft of Computer Hardware

605.3 Theft of Media Containing Sensitive Data

605.4 Incident Reporting

605.5 Security Reviews

605.6 Security Investigations

## **PART 605 - REPORTING PROCEDURES**

### **605.0 General**

This part will explain the procedures for conducting entrance and exit conferences, reporting thefts, reporting computer attacks, and conducting security reviews. The term “employee” applies to all Federal, partner, or contractor employees in the office.

### **605.1 Entrance and Exit Conference**

An entrance and exit conference will be conducted for all employees, partners, and contractors by the designated security official prior to adding or removing an employee, partner, or contractor from any computer system. All NRCS offices will implement a formal check in and check out procedure that will include at a minimum the following security items:

- (a) Physical security; e.g., access, keys.
- (b) Department Computer Center access.
- (c) Local computer access.
- (d) Telephone credit cards (FTS Manager).
- (e) Disposition of files.
- (f) Formal security debriefing.
- (g) Return of equipment, including computers and telephones.
- (h) Read and sign limited personal use policy of the agency.

When an employee is entering a new duty station, the supervisor is responsible for ensuring that these procedures are followed and that IT is notified in a timely manner to ensure that proper access is granted in accordance with the employee’s needs. All new employees, partners, and contractors will be given a copy of the NRCS Computer Security Awareness Training Guide.

When exiting a duty station, the supervisor will notify IT before the employee leaves and provide disposition instruction for all files in the employee’s account.

The following is a list of appendixes that will help supervisors, IT specialists, and users ensure that reporting procedures are implemented:

- (a) Part 615.4 is a request to add/change/delete users from computer systems. This must be completed when an employee, contractor, or district employee enters on duty and

when they leave Federal employment. This is completed by the employee's supervisor and approved by the next higher level and forwarded to the appropriate IT staff. This request is retained for the period of time required by the NRCS Records Guide.

(b) Part 615.5 is an acknowledgement of receipt of user ID that is signed by the employee, contractor, or district employee. This acknowledgement is returned to the appropriate IT specialist for retention as required by the NRCS Records Guide.

(c) Part 615.6 outlines limited personal use of Government equipment that all employees, partners, contractors, and contract/program managers must sign acknowledging that they understand their responsibilities under DR 3300-1. This acknowledgement is returned to the appropriate IT specialist for retention as required by the NRCS Records Guide.

(d) Part 615.7 is a sample of exit questions that a supervisor must complete when an employee leaves the office. This document is returned to the appropriate IT specialist for retention as required by the NRCS Records Guide.

(e) Part 615.8 is part of the exit interview process that departing employees, partners, and contractors must sign acknowledging their responsibility not to disclose sensitive USDA and NRCS data.

## **605.2 Theft of Computer Hardware**

NRCS will maintain a computer hardware inventory for each office. This inventory shall include all computer equipment, including printers, fax machines, portable devices (cell phones, personal data accessories, GPS units, laptops, or any wireless devices yet to be procured).

Any loss of computer hardware shall be reported to the immediate supervisor, who will contact the appropriate law enforcement agency and administrative officer. The administrative officer will complete the required form and notify the NRCS Security Officer. The NRCS Security Officer will be provided with an inventory of the lost property, a description of any sensitive information contained on the equipment, and a copy of all reports from law enforcement. The NRCS Security Officer will notify appropriate agencies.

## **605.3 Theft of Media Containing Sensitive Data**

Theft of any media containing sensitive data will be immediately reported to the NRCS Security Officer who will, in turn, notify the USDA Office of Cyber Security.

## **605.4 Incident Reporting**

All IT security incidents (both physical and cyber) must be reported to the local security officer. (Part 615.2 contains a list of NRCS security officers.) Local and/or state security

officers will immediately provide a brief summary of the incident via e-mail or telephone to the NRCS Security Officer or Deputy Security Officer. The local and/or state security officer must complete the Incident Response Detail Report contained in Part 615.9 within three working days and forward it to the national security staff.

### **605.5 Security Reviews**

(a) IT Review. A review of security operations will be conducted as part of a scheduled onsite national IT review. These reviews will be conducted at the State or regional level and may include a visit to a field service center. (See National IRM Manual Part 515, Information Resources Management Reviews; General Manual Title 110, Part 403, Administrative and Information Technology Functional Reviews; and General Manual Title 340, Part 404, Evaluations, for policy relating the reviews.)

(b) Annual Security Review. An annual security review will be conducted in each office by February 15 of each year in accordance with policy in the National IRM Manual, Part 502, Subpart C. Part 615.10 of this handbook is the checklist that must be used for this review. A copy of each annual security review will be sent to the next highest security level. The State IT specialist will provide a State summary to the NRCS Security Officer and regional office IT person. The purpose of the review is to validate that the safeguards in place are adequate to prevent, detect, and/or recover from security failures or a disaster. The results of the security review will be used to update the Contingency portion of the Security Plan for each facility. (See Part 606 for information on Security Plan preparation.)

### **605.6 Security Investigations**

Security investigations are conducted on employees commensurate with their position sensitivity, level of access, and need to know. Employees include permanent and temporary NRCS employees, contractors, and personnel such as conservation district employees accessing NRCS computer systems. Security investigations will be processed by the supporting Human Resources Staff upon recommendation of the State security officer. The National IRM Manual, Part 502, contains policy relating to security investigations. The following table, taken from the National IRM Manual, outlines the various security clearance levels.

**Table 2 - Security Investigation Levels**

<b>Personnel</b>	<b>Security Investigation Level</b>	<b>Periodicity (years)</b>
All Employees (including IT personnel not listed below, volunteers, partners, and contractors)	National Agency Check with Law and Credit (NACLC).	10
Non-supervisory System Administrators	Limited Background Investigation (LBI).	5
Supervisory System Administrators	Background Investigation (BI).	5
Program Managers	Limited Background Investigation (LBI).	5
Technical Help Desk Personnel	Limited Background Investigation (LBI).	5
Program Help Desk Personnel	National Agency Check with Law and Credit (NACLC).	10
Security Staff and Organizational Security Officers	Background Investigation (BI).	5
Financial Personnel (05XX series)	National Agency Check with Law and Credit (NACLC).	5
Personnel Staff	National Agency Check with Law and Credit (NACLC).	5
Contracting Officers	National Agency Check with Law and Credit (NACLC).	5

**PART 606 - ANNUAL SECURITY PLAN**

606.0 Introduction

606.1 Scope

606.2 Security Plans

## **PART 606 - ANNUAL SECURITY PLAN**

### **606.0 Introduction**

This part provides standards, guidelines, procedures, and responsibilities for developing and administering Information Technology (IT) resources at the service center, State, and regional levels. Each office must complete an annual security review, a business continuity plan, and a risk assessment. These documents must be reviewed annually and revised if major modifications to the system or site occur. The three documents will be used to develop the annual security plan. The security plan must address any deficiencies identified by the security review, list any security accomplishments in the prior year, and any anticipated actions for the coming year.

It is the responsibility of the local, State, and regional security officers, in conjunction with the system administrators, to complete the security plans. The field service centers will forward a copy of the site security plan to the appropriate State security officer.

Part 615.10 is a template that can be used to complete a section of the Annual Security Plan. (See Part 606.2 for a complete listing of all components of a Security Plan.)

In accordance with OMB Circular No. A-130, Appendix III, Revised, Security of Federal Automated Information Systems, each general support system and major application will develop a security plan consistent with guidance issued by OCIO and NIST. For offices that develop applications, the Computer Security Act of 1987 mandates that agencies develop computer security plans for all sensitive systems and have the systems certified and accredited.

### **606.1 Scope**

Procedures in this handbook apply to all operational levels of NRCS. The provisions in this handbook are intended to protect all IT assets of the agency, including the following:

- (a) Computing and word processing equipment and peripherals.
- (b) Computer programs.
- (c) Data or information.
- (d) Related documentation.
- (e) Contractual services.
- (f) Personnel.
- (g) Supplies.

- (h) Facilities

## 606.2 Security Plans

Although various offices may have different IT configurations, basic requirements are the same for all offices. This Part provides guidelines for developing the annual security plan which must include the following:

- (a) Security Review. See Part 605.5(b) for a discussion on security reviews.
- (b) Risk Assessment Plan.

(1) The Risk Assessment Plan documents the computer security controls and procedures used in NRCS offices to protect computer equipment, data, automated information systems, and information resources from unauthorized access, use, modification, or disclosure. When completed, the checklist will provide an overall security assessment of the office that may be used in audits and investigations. Requirements of the Risk Assessment Plan are met by completion of the Annual IT Security Review and Risk Assessment (Part 615.10).

(2) Regional, State, and field offices must conduct a comprehensive risk assessment of the total office environment, including computer resources. The assessment will consider the following:

- (a) Identification of the risks and vulnerabilities that exist and the protective measures to offset the risks.
- (b) Ability of the office to perform its missions and tasks correctly and in a timely manner under conditions that could adversely affect its physical environment, personnel, information resources, and essential data.
- (c) Probability that each adverse event will occur.

- (c) Business Continuity Plan.

(1) Business Continuity Plans are a vital part of the overall security plan and must be comprehensive and effective. The Business Continuity Plan should minimize the damage caused by unexpected and undesirable occurrences or contingencies that interrupt the normal operations of a facility. Instructions and a template for completing a Business Continuity Plan are in Part 615.11.

(2) A Business Continuity Plan describes the actions the office shall take, the resources the office shall use, and the procedures the office shall follow before, during, and after an undesirable occurrence interferes with a function that supports a critical product or service.

(3) An effective Business Continuity Plan must accomplish the following major objectives:

- (a) Keep minor problems from becoming major problems.
  - (b) Keep major problems from becoming catastrophic problems.
  - (c) Allow effective response and recovery from unexpected and sudden disruptions of operations.
  - (d) Permit the response and transition of critical work to other facilities or to a different mode of operation in a timely manner.
  - (e) Reduce the damaging consequences of unexpected, unfortunate, and undesirable occurrences, regardless of their magnitude.
- (d) Certification and Accreditation Document. Every computer system application and/or software developed for statewide, regional, or national distribution shall be certified by the “owner” or sponsor before placing that “system” or application into production. This certification will consist of acceptance testing performed independent of the developer. The sponsor shall review all vulnerabilities and proposed safeguards to assess the individual and collective adequacy and acceptability of the overall system certification.

**PART 607 – ESTABLISHING A LOCAL AREA NETWORK**

607.1 Acquiring Necessary Hardware/Software

607.2 Space Security

607.3 Telecommunications

607.3 Strategies to Reduce Risk

## **PART 607 – ESTABLISHING A LOCAL AREA NETWORK**

### **607.1 Acquiring Necessary Hardware/Software**

All hardware and software must be purchased using the procedures established with Telecommunications Operations (T-OPS) and CCE.

### **607.2 Space Security**

Local area networks will not allow public access without approval.

Servers, routers, hubs, and patch panels shall be located in a secure area with limited access.

### **607.3 Telecommunications**

All unused data lines shall be disconnected from the LAN.

If non-static addressing is used, a log shall be maintained to link from machine to IP. These logs must be maintained for at least one year.

IP blue prints shall be kept secured.

### **607.3 Strategies to Reduce Risk**

The following are some strategies that will reduce the risk of local area network compromises.

- (a) Investigate the occurrence of an external IP address performing activity on internal network servers.
- (b) Question remote users who try to execute system services that are not actively executing on the servers.
- (c) Domain Name Service updates must not be permitted from unknown or external network sources.
- (d) Monitor network access to internal host computers by external sources.
- (e) Remote logon procedures must not be stored on WWW or FTP servers.
- (f) Audit logs must not be stored on WWW or FTP servers.
- (g) Audit and system logs must be transferred from WWW or FTP servers daily.

(h) Sensitive data must not be stored on WWW servers or publicly accessed computers.

**Part 608 – BUSINESS CONTINUITY PLAN**

608.0 – General

608.1 Purpose

608.2 Preparation of Business Continuity Plan

608.3 Contents of Business Continuity Plan

608.4 Documentation of Business Continuity Plan

## Part 608 – BUSINESS CONTINUITY PLAN

### 608.0 – General

Business continuity planning is an essential element of information security.

### 608.1 Purpose

(a) The primary purpose of the Business Continuity Plan is to provide for the protection and restoration of IT facilities and capabilities, and to reduce the damaging consequences of any unexpected or undesirable event. Business Continuity Plan strategies and procedures apply to all operations in the office. It would be extremely difficult and poor management practice to isolate the automated activities and limit the Business Continuity Planning to those activities.

(b) The loss of operational capability may be caused by many types of occurrences, including

- (1.) Disasters such as fires, floods, power failures, wind and ice storms, tornadoes, and earthquake.
- (2.) Sabotage.
- (3.) Carelessness.
- (4.) Strikes and other civil disorders.
- (5.) Accidents.

(c) A comprehensive Business Continuity Plan not only reduces the severity of the effects of undesirable occurrences, it also permits responding in a timely manner and eventual effective recovery.

(d) Preparing a Business Continuity Plan provides an excellent opportunity to identify and minimize potential problems that could disrupt operations.

(e) Business continuity planning should not be directed solely at reacting to major catastrophes. The probability of an undesirable event occurring is generally inversely related to its magnitude.

- (1) Usually, the greater the catastrophe, the lower the probability that it will occur.
- (2) Small problems disrupt normal operations at a far higher frequency than do large problems.

(f) The primary goal is to keep the office in operation. If that is not possible, the goal is to restore operations as quickly and as smoothly as possible.

## 608.2 PREPARATION OF BUSINESS CONTINUITY PLAN

### A. Security Review.

The security review section of the office security plan provides a basis for developing a Business Continuity Plan that covers all needs of the office. All office resources and functions are not equally important to the total operation and equally susceptible to harm or interruption. A properly performed security review provides an awareness of the following:

- (1) Functions that are supported by each resource element, such as devices, programs, and data.
- (2) Susceptibility of each element to accidental or intentional harm and the consequences of such harm.

The Business Continuity Plan is based on the following:

- (1) An awareness of the relative dependence of the office on each of its component parts.
- (2) A general knowledge of the probability that an undesirable occurrence could happen to each component.
- (3) A determination of the consequences of an undesirable occurrence and actions necessary to minimize the chances of the occurrence, the loss of capability if it does occur, or both.

### B. Critical Dependencies.

The critical dependencies section of the office security plan lists the specific resources required for the office to recover from a loss of operation. The prompt recovery from a loss of capability depends on the availability of backup or replacement resources. The specific resources required for recovery depend on the type of problem causing loss of capability. Some of the resources essential to reestablish operations warrant special care to ensure their continuing availability and the early recognition of a loss of capability. Critically dependent resources are usually in either of the following distinct categories:

#### 1. Resources under the direct control of the office management.

Place special emphasis on determining the data that is needed for backup and recovery purposes.

- Clearly identify vital information to ensure that it is available. Accordingly that information should have the first priority in any emergency situation.
- Categorize and maintain the data that is extremely useful to the organization and very costly to regenerate.

Although the primary concern is critical data, consider other resources, including:

- Any required office equipment in addition to the computer.
- Not readily attainable office supplies.
- Blank forms required for necessary processing.
- Alternate office space.

## **2. Resources under the control of other persons**

Resources controlled by others include:

- Replacement computer equipment.
- Computer programs and other software.
- Communications facilities.
- Equipment and supplies that are not maintained in on offsite location.

Place particular attention on acquiring firm commitments for offsite storage facilities and alternate site processing agreements. Review the external commitments of critical resources frequently to ensure that they are available.

## **C. Emergency Response Planning.**

Emergency response planning refers to the actions that the office must take immediately after an emergency occurs to protect life and property and to minimize the effects of the emergency. The security review can provide a basis for developing a loss control plan. Emphasize the threats that are most likely to occur and have the potential for the greatest impact. The loss control plan must:

- Define the steps to be taken.
- Assign responsibilities for general and specific steps.
- Provide needed materials and equipment in convenient locations.

Offices must develop and maintain a separate list of actions for each of the defined risks.

- Plan specific actions because different occurrences will require different responses; for example, a major fire will require immediate, emergency action but a power outage may allow ample time to take all necessary actions.
- Enforce extreme precautions to protect the individuals involved from possible harm or injury.

## **D. Backup Operations Planning.**

The security review must identify the situations that need backup operations to avoid costly delays in accomplishing the mission of the office. The next step is to develop plans for backup operations that are economically, technically, and operationally sound. The details of the backup plan will be site specific; however, the guidelines in this subparagraph apply to all offices. Two elements that are vital to developing a backup plan are:

## National Information Security Handbook

- (1) Acquiring a safe, secure, and convenient location for offsite storage of critical material.
- (2) Establishing backup computer capability.

The offsite storage must be in a location that provides safe and secure storage for the sensitive data. Diskette and magnetic tape storage:

- Shall be in a controlled environment consistent with the requirements of the vendor, especially temperature and humidity.
- Shall be convenient and accessible during normal office hours.

Consider the natural disasters that pose a threat to the office; for example, whether the office is in a location that is subject to flooding. The offsite storage location must not be in that area. Potential offsite storage locations include:

- Federal offices.
- State or county government offices. The county courthouse is usually a good option.
- Commercial locations with a secure safe or vault, such as financial institutions or insurance offices.
- Other data processing facilities in the area if it is possible to arrange a reciprocal agreement for offsite storage.

The State office has several options for a backup computer facility, including:

- Neighboring State Offices have compatible computer configurations that may be used in an emergency.
- Some county offices have computers large enough to process a majority of the State applications.
- The computer vendor may have compatible computers within a reasonable distance of the State Office.

The county office has several options for a backup computer facility, including:

- Neighboring county offices have compatible computer configurations that may be used in an emergency.
- The State Office.
- The computer vendor may have compatible computers within a reasonable distance of the county office.

Offices should not restrict themselves to a single backup site. If the only backup agreement is with a neighboring location, both locations could be out of operation from a widespread natural disaster, such as a hurricane, earthquake, or windstorm. Offices should have a primary backup agreement with a nearby facility and a secondary agreement with another facility.

Office managers should ensure that arrangements have been made for backup computer processing with a compatible facility. These can be reciprocal agreements that will help out both organizations.

Offices should develop several forms of the backup plan, including:

- A “worst case” plan for when the office suffers total destruction.
- A minimum duration plan, for a relatively minor and short duration interruption.
- Plans for one or more operating periods between minimum duration and worst case.

Although offices should tailor individual plans for specific occurrences and the projected duration of backup operations, there will be many similarities between the plans. A recommended approach is to first make a detailed plan in case of total destruction because that is the most demanding situation. Offices can scale down or modify the total destruction plan for the less demanding situations.

## **E. Developing Backup Operations.**

Consider the following specific areas when developing the backup plan:

### **(1) People.**

The people who will be involved in the operation are the most important element in any plan. No other element in the plan has the flexibility, adaptability, and versatility provided by the people involved in the operation.

- a. The plan must document specific responsibilities for office personnel. Management must ensure that employees who have been assigned specific responsibilities:
  - Are aware of the assignment.
  - Have the necessary experience and training to fulfill the assignment.

- b. A widespread disaster, such as a flood, tornado, or hurricane, will cause personal problems for office employees that:
  - They will have to take care of before they can help the office.
  - Will have a major impact on office recovery.

## **(2) Data.**

The security review must identify the data that requires specific protection and is essential to the operation of the office. Loss or unauthorized modification of critical data is probably the most frequent cause of operational interruptions.

- a. Offices must:
  - Periodically copy critical data and store it in a secure, offsite location, according to the office security plan.
  - Regularly copy critical data; however, the frequency of the copy process depends on the activity with the data.
  - Perform additional copy cycles if there is an unusual amount of activity with the data.
- b. Offices should consider the difficulty of attempting to update the backup data to reflect the current status. The more difficult this process, the more frequently the data should be backed up.

## **(3) Software.**

Software, such as computer programs, constitute a special type of data. Software tends to be more stable than data; however, software is sufficiently subject to change that offices must exercise care to sufficiently protect current versions and all necessary supporting documentation. In the event of total destruction, call the Help Desk.

Offices should still maintain duplicate copies of all applications programs and operating software in a secure, local, offsite location. This offsite backup will enable the office to resume operations quickly in the event of a minor or localized emergency.

## **(4) Equipment.**

Office equipment is the most readily replaceable of the office assets. The computer equipment will be a little more difficult to replace, but it should not present a problem. The maintenance contract with the computer vendor should:

- Provide for repairing and replacing computer equipment.
- Indicate the amount of time required to replace the computer equipment.

Offices should discuss emergency equipment replacement with the office equipment supplier, the State Office, or local vendors. After these discussions, offices can estimate the amount of time required to replace the required equipment, and include these estimates in the Business Continuity Plan.

### **(5) Communications.**

Although internal operations may not require a communications system, it is necessary for interaction between State and County Offices, Fort Collins, and National Headquarters. Arrange an alternative means of communications with other offices for temporary and extended periods of loss of communications.

### **(6) Supplies.**

Except for a few items that might be unique to a particular office, most supplies are catalog items that are readily available. Offices should:

- Plan to stockpile enough supplies so that normal operations can continue in the event of a problem of any kind.
- Consider an offsite, backup supply in the event of damage to the office or other causes of a shortage of supplies.

### **(7) Space.**

If a disaster makes the office space unusable, the office must arrange to obtain new office space. Ideally, any move should be into a permanent location. Offices must plan for space:

- That can be used temporarily while the original site is being rehabilitated.
- To relocate operations with relative permanence.

### **(8) Documentation.**

One of the most critical but neglected elements of any operation is adequate and usable documentation. Maintain a complete set of all pertinent documentation and a copy of the Business Continuity Plan in the offsite storage facility. A neighboring county office can serve as a backup source of necessary documentation, such as handbooks, manuals, or directives. In an emergency, personnel will:

- Be performing tasks and duties for which they are not normally responsible.
- Need proper documentation to help them perform unfamiliar assignments.

## **(F) Recovery Planning.**

Offices must consider the backup operation when they develop their recovery strategy because their recovery actions may:

- Overlap the backup operating procedures.
- Be the next step after backup operations to restore the office capability after partial or complete destruction of the facility or other resources.

Offices must prepare a plan for recovery from total disaster, and then develop from that plan the procedures for situations of less than total disaster.

If the office facility has been destroyed and the office is temporarily functioning at the backup or alternative site, use the following steps to recover normal office operations:

- a. Locate and obtain enough office space to house all necessary operations. The following are the three basic options for this step:
  - Repair or restore the current facility.
  - Rebuild the current facility.
  - Build or acquire a new facility at a different location.
- b. Perform the required modifications to the selected location, including adding or changing the following:
  - Partitions.
  - Electrical service.
  - Required communications facilities.
  - Air conditioning.
  - Security.
  - Fire safety.
  - Other special requirements.
- c. Obtain and install IT equipment.
- d. Procure needed supplies, office equipment, furniture, and other operational necessities.
- e. Verify that all needed equipment, supplies, and materials have been installed and are in good working order.
- f. Transfer operations from the backup site to the permanent facility.

The more preliminary preparation that can go into this plan, the simpler it will be to carry out. At a minimum, offices should research the necessary activities and prepare a broad outline of required actions.

## **G. Testing Business Continuity Plans.**

Testing and evaluating the Business Continuity Plan is one of the most important aspects of successful Business Continuity Planning. Since emergencies do not occur very often, it will be difficult to ensure the adequacy and proficiency of personnel and plans without regular training and testing. Therefore, it is important to plan and budget for both.

A relatively simple procedure for testing the availability and adequacy of backup files is to attempt to perform a particular task by using only the assets available at the offsite storage location.

Testing the fire fighting, loss control, evacuation, bomb threats, and other emergency procedures must:

- Ensure that plans are adequate and workable.
- Provide an opportunity to train personnel.

### **608.3 CONTENTS OF BUSINESS CONTINUITY PLAN**

The Business Continuity Plan shall follow the outline of topics in this paragraph. Although individual circumstances vary from office to office, the outline is general enough to adapt to the needs of each office.

#### **A. Statement of Purpose.**

##### **1. Purpose and Scope.**

Briefly state the purpose of the plan and the office operations it covers.

##### **2. Assumptions.**

List any pertinent assumptions about the office operations or the coverage by the plan.

#### **B. Responsibilities.**

##### **1. Preparation of Business Continuity Plan.**

Indicate who is responsible for preparing the Business Continuity Plan.

##### **2. Maintenance of the Plan.**

Indicate who is responsible for maintaining and updating the Business Continuity Plan.

**C. Backup and Recovery Actions.**

List the procedures for:

1. Data Protection and Retention.
2. Data Recovery.
3. Equipment Recovery.

**D. Disaster Recovery. List:**

1. Emergency Responses.
2. Backup Operations.
3. Recovery Actions.

**608.4 DOCUMENTATION OF BUSINESS CONTINUITY PLAN**

The Business Continuity Plan shall be a permanent part of the office records. Review and update the plan annually or as needed. Complete the Business Continuity Plan checklist after the annual review of the Business Continuity Plan. This provides the basic information for the office Business Continuity Planning process.

## A. Business Continuity Plan Example

### 1 Statement of Purpose

- A. Purpose and Scope This Business Continuity Plan has been developed to provide guidelines for all office employees when an unexpected or undesirable event occurs that disrupts the normal operations of this office. The procedures and techniques are intended to reduce the probability of undesirable event occurrence, minimize the severity of the effects of an unpreventable disruption, provide a timely response to an emergency, and provide an effective and timely recovery.
- B. Assumptions This Business Continuity Plan applies to all activities and operations in the State Office. The plan is intended to provide protection for all information resources in the office, whether automated or manual.

### 2 Responsibilities

- A. Responsibilities of State IT Security Officer
- Preparing the State Office Business Continuity Plan.
  - Maintaining and updating the plan. However, other staff members will have specific responsibilities for the plan and will contribute to the overall effectiveness of Statewide Business Continuity Planning.

### 3 Backup and Recovery Actions

- A. Data Protection and Retention Procedures
- All automated files are copied periodically. The normal schedule for backup is weekly, as a scheduled Friday afternoon activity. However, if any file has a higher than normal rate of activity, that file is copied more often at the discretion of the responsible Program Specialist.
- The backup files are stored at [indicate site where files are stored]. As part of a reciprocal agreement, the backup files from the County Office are stored in the State Office.
- The files that are copied for backup purposes include all master data files, application program files, and system software files.
- All backup files are logged in and out of the backup storage facility.
- B. Data Recovery Procedures
- If the current data contained in the computer is lost, the backup files will be used to restore the system. Any transactions that have occurred since the time of the last backup will be entered into the system to finish the complete restoration of the data files.
- C. Recovery Procedure for
- If any of the IT equipment needs to be replaced because of an emergency or disaster condition, the State Office will be notified

Equipment and  
Supplies

immediately.

Other office equipment that needs to be replaced will also be ordered immediately. On a temporary basis, some equipment may be borrowed from, or shared with, other offices.

## 4 Disaster Recovery

### A. Emergency Responses

An emergency evacuation plan for the office has been published and distributed to all employees.

One person, as well as an alternate, has been assigned responsibility for the IT equipment in emergency situations. If time permits, this person will perform an orderly shutdown of the computer following the procedure established for this process.

If there is not time for an orderly shutdown, the power to the CPU and air conditioning will be shut off as the building is evacuated.

The primary consideration in all emergency situations is the desire to protect the individuals involved from possible harm or injury.

### B. Backup Operations

Arrangements have been made with another office to use those computer facilities if the State Office is unable to operate. [Please indicate which office this agreement has been made with.]

Since the service center will have a limited amount of computer time available during the normal day shift, especially during peak times of the year, the agreement specifies that the State Office applications will be processed during the evening shift with State Office employees operating the equipment during that time.

A five-day supply of essential forms, other material, and supplies unique to the State Office is stored in [list office]. Other office supplies and material will be provided by the service center until such time as emergency requisitions can be fulfilled.

A copy of this plan is stored in the service center, and another copy is kept at the State IT Security Officer's home.

### C. Recovery Actions

A Disaster Recovery Team has been composed of key office personnel. This team will go into operation as quickly as possible after the emergency occurs. An emergency notification list with Disaster Recovery Team members will be provided to the State Conservationist.

When the team has determined the extent of the disaster, the appropriate sections of the Emergency Recovery Plan will be implemented, and all employees will be notified of the status of the situation, as well as what their next actions should be.

**5 Appendices to the Business Continuity Plan**

A. Appendices This table lists appendices to the State Office Business Continuity Plan.

Appendix Number	Title	Description
1	Emergency Building Evacuation Plan	Details to be determined by each office.
2	Emergency Computer Shutdown Procedure	
3	Emergency Telephone Network	
4	Inventory of OffSite Materials and Supplies	Each office will determine and list materials and supplies that are to be stored in the backup location.
5	Disaster Recovery Team	Details to be determined by each office.
6	Emergency Recovery Plan	

**Part 615 – Glossary**

[615.0 Definitions](#)

[615.1 Commonly Asked Questions](#)

[615.2 NRCS IT Security Officers](#)

[615.3 Training Certification Security Awareness Training](#)

[615.4 Request to Add/Change/Delete Employee on Computer System](#)

[615.5 Acknowledgement of User ID](#)

[615.6 Limited Personal Use](#)

[615.7 Exit Interview Questions](#)

[615.8 Security Clearance Exit Interview](#)

[615.9 Federal Computer Incident Responses Capability \(FedCIRC\) Detail Report](#)

[615.10 Annual IT Security Review and Risk Assessment](#)

**Part 615 – Glossary****615.0 Definitions**

Access	The ability to do something with a computer resource (e.g., read, create, modify or delete a file, execute a program, or use an external connection).
Application	A program or system that allows you to process certain types of data.
Audit Trail	A technical mechanism that assists the security officer to ensure individual accountability of system users. Users are less likely to attempt to circumvent security policy if they know their name will show up in an audit log.
Automated Information System (AIS)	Any equipment of an interconnected system to subsystems that is used in the automatic acquisition, storage, manipulation, control, display, transmission, or reception of data and includes software, firmware, and hardware.
Authorization	The permission to use or access a computer resource. Permission is granted, directly or indirectly, by the application or system owner.
Backups	Media stored on tapes or diskettes and maintained in an offsite location to be used to restore an automated system in the event of a disaster.
Cookie	<p>A small piece of information that may be sent to a computer connected to the Internet to track a user's Web browsing habits. There are two types of cookies:</p> <p>Session Cookie – A line of text temporarily stored in a computer's Random Access Memory that is never written to a drive and is destroyed as soon as the browser is closed.</p> <p>Persistent Cookie – A more permanent line of text that is saved by a browser to a file on the hard drive and can be used to track a user's browsing habits. NOTE: Persistent cookies will not be collected or used at any USDA Internet or Intranet Web site or by contractors operating Web sites on behalf of USDA. Exceptions to this policy require a waiver request, which must be submitted to the Associate CIO for Cyber Security with a statement of</p>

National Information Security Handbook

	purpose and a strong justification.
Client	A computer used to request and retrieve information from another computer on the network.
Computer System	One or more computers and attached peripherals that may be connected to other computers by a telecommunications network.
Confidentiality	Assurance that sensitive data are kept private and are accessible only by authorized personnel on a need-to-know basis.
Denial of Service (DOS)	Action(s) that prevent any part of an AIS from functioning in accordance with its intended purpose. These attacks flood portals to online computers with malicious intent, denying access to those having legitimate need for access.
Domain	A collection of computers on the network that share a common directory database on the primary server computer.
Domain Name Service (DNS)	A hierarchical method of naming network host computers on the Internet. For example, the “.gov” domain has “.usda” as one of its subdomains.
Federal Computer System	The Computer Security Act of 1987 defines a “Federal computer system” as a computer system operated by a Federal agency, by a contractor of a Federal agency, or any other organization that processes information on behalf of the Federal Government to accomplish a Federal function.
File Transfer Protocol (FTP)	Enables users to copy files to or from other computers on the Internet.
Firewall	A combination of hardware and software that has as its sole purpose the protection and isolation of an interior network from outside threats. Modem connections bypass firewalls and any other cyber security measures and are considered potentially serious breaches.
Homepage	The first page (i.e., the opening screen) of a Web site – www.usda.gov.
Intranet	A “localized” network of computers used to communicate electronically.
Internet	A global “network of networks” used to communicate electronically that is linked by a common set of protocols. These protocols allow computers from one network to communicate with

	a computer on another network.
Internet Protocol (IP)	The protocol that enables information to be routed from one network to another in packets and then reassembled into information when the packets reach the destination computer.
IP Address	An address scheme that uniquely identifies networked computers that are used to access the Internet.
Log File	A file that contains functions and activities performed by the computer.
Network File System (NFS)	A distributed file system that allows a person to work with files on a remote host as though working on the actual host computer.
Offsite Storage	Any place physically located a significant distance away from the main processing environment, such as a locked box at the bank, another office several blocks or miles away from the primary site, or in another State. Magnetic media shall be maintained in a temperature-controlled offsite environment.
Protocol	A set of rules for information to transferred over the network so that your computer will know what to do when it receives the information from another computer.
Security Awareness	An initiative that sets the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of security failure. Further, awareness reminds users of the importance of security and the procedures to be followed.
Sensitive Data	Any information, which through loss, unauthorized access, or modification could adversely affect the national interest, the conduct of Federal programs, or the privacy of individuals (which is protected under 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.
TCP/IP	Transmission Control Protocol/Internet Protocol. The suite of protocol Internet use is based on.
Telnet	A TCP/IP service that allows a user to establish an interactive terminal session with a remote host.
Trojan Horse	An apparently useful and innocent program containing additional hidden code that allows the unauthorized collection, exploitation,

	falsification, or destruction of data.
Virus	An unauthorized program that replicates itself and spreads onto various data storage media (diskettes, disks, magnetic tapes, etc.) and/or across a network for malicious intent. The symptoms of virus infection include considerably slower computer response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of computers.
Virus Signature	A unique set of characters that identify a particular virus "family." This may also be referred to as a virus marker.
Virtual Private Network (VPN)	A network that uses encryption and authentication to build secure private tunnels over public networks.
Web Browser	Software that allows a user to locate, view, and access information on the Internet by the use of a graphical interface.
World Wide Web (WWW)	A network that offers access to Web sites all over the world using a standard interface for organizing and searching.
Worm	A complete program that propagates itself from system to system, usually through a network or other communication facility. Similar to a virus, a worm can infect other systems and programs. Unlike a virus, a worm does not replicate itself. A worm copies itself to a workstation over a network or through a host computer and then spreads to other workstations. It can easily take over a network as the "Internet" worm did. Unlike a Trojan horse, a worm enters a system uninvited.

### 615.1 Commonly Asked Questions

Users must be aware that personal information that traverses the Internet and Intranet is not secure and that data integrity cannot be guaranteed. Also, the Government is in no way responsible for personal data that is “sniffed” (by Network Protocol Analyzer, commonly known as a “sniffer”) from the Internet or the Intranet and used for unauthorized personal gain or embarrassment to the user. Users use the Internet at their own risk for personal business.

This short overview is intended for managers, supervisors, employees, partners, and contractors to use as a guideline for managing and enforcing departmental and agency policy. It is not intended to override or replace this policy. It also is not intended to override or replace the “Standards of Ethical Conduct for Employees of the Executive Branch” handbook, codified in Title 5, Code of Federal Regulations, Part 2635 (5 CFR 2635). It should be used as a “question and answer” document to help clarify the intentions of this agency policy.

<b>Commonly Asked Questions</b>	<b>Guidelines To Follow</b>	<b>General Comments</b>
1. May I use a private Internet Service Provider (ISP) like AT&T or America On-Line (AOL) from my office work station to access the Internet during business hours or on my own time?	No. All access to the Internet must be through the USDA Internet Access Network. No private Internet Service Providers, such as AOL, are allowed.	Provisions have been established for special testing scenarios at development centers of Web pages. However, a waiver from the security office to the Department is required.
2. Do I need any special permission to use Government equipment for limited personal use on my own time?	Yes. Employees, partners, and contractors must request “limited use access” from their immediate supervisor for specific time frames, such as before or after work and/or during specified lunch periods and/or breaks to use the Internet for personal use.  The supervisor may approve or deny any request.	It’s the supervisor’s decision if they want the request verbally or in writing.  The limited personal usage must comply with the intent of DR 3300-1. Supervisors should make sure that all employees, partners, and contractors have access to this DR and are strongly encouraged to read it.
3. May I use Government- owned	No. If employees or partners choose to use	Buildings or separate offices that have 24-hour guard

<b>Commonly Asked Questions</b>	<b>Guidelines To Follow</b>	<b>General Comments</b>
equipment any time after hours for limited personal usage?	<p>Government equipment before and/or after work hours, it should conform to reasonable building opening and closing timeframes to ensure that all building security regulations are followed and that the Government incurs no additional cost.</p> <p>For example, if the normal business hours of operation at the employees workplace are from 6 a.m. to 8 p.m., it is not reasonable to allow employees to come in earlier than 6 a.m. or stay later than 8 p.m. to use government equipment for limited personal use.</p>	<p>services would follow normal building security regulations of signing in and out after hours.</p> <p>Most Government offices have posted standard business hours of operation. Use of Government equipment outside these hours is by permission only.</p> <p>Union agreements clearly define normal Government business hours for a standard workday.</p>
4. May my immediate family members or friends use the Government equipment after hours?	No. Only Federal employees, partners, and assigned contractors are allowed to use Government equipment for limited personal use.	
5. May Federal Government contractors and partners use Government equipment for limited personal use?	Yes. Contractors and partners are governed by the same set of rules as Government employees. However, in the case of contractors, prior permission for use must come from the Contracting Officer's Representative (COR) or Contracting Officers Technical Representative (COTR).	The letter of the contract and statement of work are always the determining factors for contractors and this privilege will be disallowed if so stated in the contract language.
6. What are some specific things that I	Some examples of items that you cannot do:	There are several obvious things for which

<b>Commonly Asked Questions</b>	<b>Guidelines To Follow</b>	<b>General Comments</b>
<p>cannot do while using the Internet or e-mail for limited personal use.</p>	<p>that you cannot do:</p> <ul style="list-style-type: none"> <li>Run a private business.</li> <li>Use the equipment as a staging ground or platform to gain unauthorized access to other systems.</li> <li>Create, copy, transmit, or retransmit chain letters or other mass mailings regardless of subject matter.</li> <li>Solicit, advertise, or sell items using such services as E-bay or run a real-estate office.</li> <li>Send electronic messages containing discriminatory language or remarks that may constitute sexual harassment.</li> <li>Make use of sexually explicit materials or remarks that ridicule other coworkers on the basis of race, creed, religion, color, sex, handicap, national origin or sexual orientation.</li> <li>Gamble.</li> <li>Earn outside income.</li> <li>Cause congestion, delay, or disruption of services to any Government system or equipment by sending greeting cards, videos, sound, or other large file attachments</li> </ul>	<p>Government equipment must not be used. However, much of the prohibited areas are a matter of common sense.</p>

<b>Commonly Asked Questions</b>	<b>Guidelines To Follow</b>	<b>General Comments</b>
<p>7. Can anyone see what I am doing when I send e-mail messages or use the Internet?</p>	<p>Yes. Monitoring tools are in place for security and telecommunication administrators to monitor all access to the Internet and e-mail.</p> <p>By using Government office equipment, consent to monitoring and recording is implicit with or without cause, including, but not limited to, accessing the Internet and using e-mail.</p>	<p>USDA DR 3300-1 states that employees and contractors do not have the right, nor should they have the expectation, of privacy while using Government office equipment at any time.</p> <p>Departmental and agency officials may access e-mail messages whenever there is a legitimate governmental purpose for such access. System administrators and other personnel with special system level access privileges are expressly prohibited from reading the e-mail of others unless authorization has been granted by senior management officials.</p>
<p>8. May I bring games (CD's or diskettes) from home?</p>	<p>No. Playing games in the workplace during or after business hours is prohibited.</p>	<p>You can bring music CD's from home and play at work as long as the noise does not disrupt the workplace or other employees. Earphones or headsets are strongly encouraged.</p>
<p>9. May I download games from the Internet and play them?</p>	<p>No. You may not load games on the hard drive of your PC anytime. Playing games on-line is prohibited.</p> <p>In addition, creating, downloading, viewing, storing, copying, or transmitting materials related to illegal gambling, illegal weapons, terrorist</p>	<p>Loading "nonstandard" software on any Government PC can raise questions of compatibility. Your software can conflict with one or more Government applications and cause PC and/or network problems. The presence of nonstandard software on a PC makes</p>

National Information Security Handbook

Commonly Asked Questions	Guidelines To Follow	General Comments
	activities and any other illegal activities are strictly prohibited.	technical support difficult if not impossible.
10. May I make personal banking transactions using the Internet on my own time?	Yes provided it does not require loading of software. If your bank has a Web site that can be accessed online, you may make normal banking transactions that you would be allowed to do by phone.	You must obtain limited user access permission from your supervisor.  You cannot load banking software on your PC.
11. May I use Government equipment on my own time to copy special flyers for my own home use or for charitable clubs or <u>nonprofit</u> organizations that I belong to such as Scouts, school, or PTA?	<p>Yes. You should obtain prior permission from your supervisor. You may make a very limited number of copies of documents as long as these clubs or events are nonprofit and no service fee is being charged.</p> <p>USDA-sponsored or work-sponsored teams, such as USDA bowling and/or golf leagues, may use Government equipment to print documents after hours as long as you are not being paid a salary for performing this activity.</p> <p>Also, there must be minimal additional expense to the Government.</p> <p>The intent is not for the Government to subsidize printing costs for nonbusiness-related ventures of any kind</p>	<p>You cannot store these personal files on Government equipment.</p> <p>Personal diskettes should be personally procured and checked for viruses prior to use.</p>
12. May I buy and sell	No. Neither	The intent of this privilege is

<b>Commonly Asked Questions</b>	<b>Guidelines To Follow</b>	<b>General Comments</b>
stock online on my own time?	<p>telecommunications resources nor official time shall be used to earn outside income. Therefore, these types of activities cannot be performed during work or nonwork hours.</p> <p>However, you can make changes on line to TSP accounts.</p>	to allow some limited management of your personal TSP retirement funds and is not intended to support daily stock trading.
13. May I use Government equipment to print special documents for sports teams and other <u>for-profit</u> clubs that I belong to?	No. The intent is not for the Government to subsidize printing cost for non-business related ventures of any kind	See item 11 above.
14. Will I get in trouble if I violate agency regulations regarding Internet and electronic mail?	Yes. Up to and including dismissal depending on the severity of the offense.	
15. What are the rules for downloading software from the Internet?	<p>Downloading software is not permitted whether it's free or not.</p> <p>You cannot download software from the Internet nor can you bring software in from outside of USDA that violates the copyright on the software and/or makes NRCS liable for violation of the Copyright Act.</p>	
16. May I use the telephone for personal business?	Yes. Limited personal use is allowed as long as it does not generate more than minimal expense to the Government.	Long distance personal calls are prohibited unless you use a calling card. Length of calls should be kept at a minimum.

<b>Commonly Asked Questions</b>	<b>Guidelines To Follow</b>	<b>General Comments</b>
<p>17. Are personal e-mail messages allowed to be sent and received at work?</p>	<p>Yes. You can send and receive e-mail messages within reason to and from nonbusiness addresses.</p> <p>However, you are not allowed to establish personal e-mail accounts at work using Hotmail, Yahoo etc.</p>	<p>You are not allowed to forward your personal ISP e-mail to your Government e-mail account.</p> <p>Personal e-mail containing large attachments are not authorized because of their impact on server resources.</p> <p>Please note that all e-mail, both business related and personal, will be stored and backed up nightly on the agency network.</p>
<p>18. May I customize the wallpaper and pattern on my PC?</p>	<p>Yes. Changing wallpaper is not considered to be a configuration change.</p> <p>However, employees are guided by the code of ethics and conduct and must adhere to all polices regarding offensive materials in the workplace.</p>	<p>Pictures of family, animals, and other normally acceptable business office type pictures are ok.</p> <p>See your supervisor for final determinations.</p> <p>Supervisors will direct the users to remove inappropriate or offensive wallpaper immediately from all Government equipment.</p>
<p>19. May I download screen savers from the Internet or bring a CD of screen savers from home and load it on my PC or laptop?</p>	<p>No. You may not download screensavers or any other file from the Internet.</p> <p>However, you may capture any appropriate graphic image for use as a screen saver or wallpaper from non-Government sources within the guidelines of item 18 above.</p>	<p>Installing a screen saver is considered a configuration change to the equipment and is known to cause resource problems.</p>
<p>20. Can I use the fax machine for personal</p>	<p>Yes. Within common sense and limited boundaries, you</p>	<p>You should obtain limited user access permission</p>

<b>Commonly Asked Questions</b>	<b>Guidelines To Follow</b>	<b>General Comments</b>
use?	can send a fax to a local number for personal business.	from your supervisor.
21. May I read such things as the newspaper, check the weather, look at new car Web sites, and other non-restrictive sites on the Internet on my own time?	<p>Yes. You can also access magazines and other reference materials not blocked or identified as offensive.</p> <p>You can research and review any business-related materials on the Internet during work hours as directed by your supervisor.</p>	You must obtain limited user access permission from your supervisor for nonbusiness related usage.
22. Is the agency looking at new technology on the Internet like allowing parents at work to use the Internet to check on their children at daycare?	<p>Yes. A number of daycare centers have installed cameras that are connected to the Internet to allow parents to observe their children during the day from their work computers as part of the family friendly initiative.</p>	<p>Employees would be allowed to check on children using the Internet once or twice a day, but must not leave this connection continuously open on their desktops.</p> <p>These types of Web sites are major “resource hogs” and can easily overburden a network if they are kept online continuously.</p> <p>You should obtain limited user access permission from your supervisor.</p>
23. If I have specific questions on computer security related issues, who should I call for clarification?	Please contact your State security officer or the National Security Officer.	<p>Each State Office should identify an onsite security official and a backup to address security-related issues and to coordinate responses with National Security Officer as needed.</p> <p>Violations must be reported to the onsite security officer,</p>

National Information Security Handbook

<b>Commonly Asked Questions</b>	<b>Guidelines To Follow</b>	<b>General Comments</b>
		who will coordinate with the State security officer.

**615.2 NRCS IT Security Officers**

<b>Office</b>	<b>Name</b>	<b>Telephone Number</b>
National Security Officer	Lyle Rich	(301) 504-2235
Deputy Security Officer	Mario Phillips	(301) 504-2250
Deputy Security Officer	Ed Haynes	(970) 295-5436
Alabama	Susan L. Dillard	(334) 887-4522
Alaska	Barbara Winters	(907) 761-7713
Arizona	Barbara Hood-Keller	(602) 280-8782
Arkansas	Joe L. McKeown	(501) 301-3147
California	Gary Bump	(530) 792-5902
Caribbean	Wanda Orama	(787) 766-5206 x223
Colorado	W. Esther Bright	(720) 544-2858
Connecticut/Rhode Island	Deborah Gagnon	(860) 871-4036
Delaware	Linda Lewis	(302) 678-4165
Florida	Donna Barr	(352) 338-9551
Georgia	Charles Burroughs	(706) 546-2050
Hawaii	Doug Fabrey	(808) 541-2600 x128
Illinois	Sheryl Casper	(217) 353-6621
Idaho	David Hoover	(208) 378-5785
Indiana	John Walters	(317) 290-3200 x344
Iowa	Dale Bruce	(515) 284-4392
Kansas	Richard Hager	(785) 823-4523
Kentucky	Mark Stevens	(606) 224-7366
Louisiana	Frank Ramsey	(318) 473-7764

National Information Security Handbook

<b>Office</b>	<b>Name</b>	<b>Telephone Number</b>
Maine	Dick Hunter	(207) 990-9503
Massachusetts	Cindy Cos	(413) 253-4369
Maryland	Edwin Moody	(410) 757-0861 x316
Michigan	Cathy Brothers	(517) 337-5136
Minnesota	Tom Radermacher	(651) 602-7903
Mississippi	Tom Powe	(601) 965-4182
Missouri	Chris Kendrick	(573) 876-9412
Montana	Stan Hamilton	(406) 587-6826
Nebraska	Frank Schmal	(402) 437-4025
Nevada	Doris I. Woodruff	(702) 784-5127
New Hampshire	Miranda Grynkewicz	(603) 868-7581 x108
New Jersey	Paul Congiusta	(732) 246-1171 x163
New Mexico	Sal Davila	(505) 761-4440
New York	Kevin Reynolds	(315) 477-6504
North Carolina	Thomas H. Shaw	(919) 873-2117
North Dakota	Terry L. Berogan	(701) 250-4763
Ohio	Paul DeArman	(614) 469-2061
Oklahoma	Harold C. Kane	(405) 742-1231
Oregon	Jean Trainor	(503) 414-3251
Pacific Islands	John M. Santos	(671) 472-7490
Pennsylvania	Ed White	(717) 237-2207
Rhode Island/Connecticut	Deborah L. Gagnon	(860) 871-4036
South Carolina	D. L. Glover	(803) 253-3934

National Information Security Handbook

<b>Office</b>	<b>Name</b>	<b>Telephone Number</b>
South Dakota	John J. Swanda	(605) 352-1246
Tennessee	Traci Holman	(615) 277-2538
Texas	Bev Minica	(254) 742-9955
Utah	Richard Allen	(801) 524-4582
Vermont	Fran Keeler	(802) 951-6796 x228
Virginia	David N. Smith	(804) 287-1634
Washington	Paul Taylor	(509) 323-2941
West Virginia	David Burns	(304) 284-7548
Wisconsin	Douglas Zwank	(608) 276-8732 x233
Wyoming	Ron Benton	(307) 261-6486
Water & Climate Center	Rickie Roberson	(503) 414-3065
National Business Mgt Center	Don Kapalka	(817) 509-3525
Info Technology Center	Jack Carlson	(970) 295-5455
Soil Survey Center	Kristi Hawks	(402) 437-5688
National Plants Database Center	James Bunch	(225) 775-6280
Cartography & Geospatial Center	Victor McWilliams	(817) 509-3438
East Region	Richard Kellogg	(301) 504-2320
Midwest Region	Scott Henney	(608) 224-3020
Northern Plains Region	Gerald D. Waters	(402) 437-4165
West Region	Jon Hayward	(530) 792-5727
Southeast Region	Charles Burroughs	(706) 546-2050
South Central Region	Joyce Petty	(817) 509-3304

### 615.3 Training Certification Security Awareness Training

TO: State Security Officer

SUBJECT: Training Certification Annual Computer Security Awareness Training

I certify that I have received and read a copy of the annual Computer Security Awareness Training information. I understand that it is my continuing responsibility to become familiar with and abide by all applicable Federal laws and USDA and NRCS computer security regulations.

I further understand that I can obtain advice on computer security issues and questions from the officials listed in the training materials. In addition, I understand that I may use Government time to complete the individual study course.

Date Completed \_\_\_\_\_

**For Employees and Partners:**

**For Contractors:**

\_\_\_\_\_  
Name (Print or Type)

\_\_\_\_\_  
Name (Print or Type)

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Organization Unit

\_\_\_\_\_  
Contracting Company/Firm

\_\_\_\_\_  
Mailing Address

\_\_\_\_\_  
Contract Number

\_\_\_\_\_  
Telephone Number

\_\_\_\_\_  
Telephone Number

### 615.4 Request to Add/Change/Delete Employee on Computer System

Choose one:    Add            \_\_\_\_\_    Requested By:    \_\_\_\_\_  
                  Change        \_\_\_\_\_    Date:            \_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
                  Delete        \_\_\_\_\_    Approved by:    \_\_\_\_\_  
Effective Date:    \_\_\_/\_\_\_/\_\_\_    Date:            \_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_

Name (Last, First, MI): \_\_\_\_\_

Previous Staff /Position/Location: \_\_\_\_\_  
\_\_\_\_\_

If leaving office or NRCS, please fill out Exit Interview Form

If new employee, will employee need files from previous employee? (Y/N) *If yes,*

Where are the files located? \_\_\_\_\_

If changing staff or coming from other office, does the employee want files transferred?  
(Y/N) \_\_\_\_\_ *If yes please specify,*

From: \_\_\_\_\_ To: \_\_\_\_\_

Are there special software needs? (Y/N) *If yes, please list*

\_\_\_\_\_

Are there special requirements needed? (Y/N) *If yes, please indicate*

\_\_\_\_\_

Level of UNIX NT or Windows knowledge \_\_\_\_\_

Does the employee need a government calling card? (Y/N)

FOR IT USE ONLY	
Login id:	_____
Home Directory:	_____
Group Name:	_____
Default Printer:	_____
Shared Directory:	_____

Individual adding/changing/deleting login: \_\_\_\_\_

National Information Security Handbook

Date Completed: \_\_\_\_/\_\_\_\_/\_\_\_\_

IT staff will retain this form in accordance with the NRCS Records Guide.

### 615.5 Acknowledgement of User ID

Listed below is the user ID requested for you by your supervisor. Please ensure that you read and understand the information below concerning your user ID.

- **I am responsible for reading the National Information Security Handbook.**
- I understand that I am responsible for protecting my password(s). I will comply with all applicable systems, security standards, and Privacy Act provisions. **I will not divulge my password(s) to any person.**
- I understand that it is a Federal crime for me to access or to allow anyone, without authorization, to access a computer operated for or on the behalf of the U.S. Government. I understand that it is a Federal crime to use, modify, destroy, or disclose information or data contained on computer systems. **This crime is punishable by imprisonment and/or fines.**

ID'S NOT USED WITHIN THIRTY (30) DAYS ARE SUBJECT TO REMOVAL.

_____	_____
Signature	Date
User id	_____
Password	_____

Please test this id within five (5) days. If the ID does not allow access, please contact your local security officer or system administrator.

Return this signed form to your IT staff for retention.

## 615.6 Limited Personal Use

**Use.** DR 3300-1, Telecommunications & Internet Services and Use, authorizes the limited personal use of telecommunications resources by USDA employees in the workplace on an occasional basis, with prior supervisory approval, provided that the use occurs during the employees' nonwork time, involves minimal expense to the government, and does not interfere with official business. Government office equipment, including information technology, includes, but is not limited to, the following: personal computers and related peripheral equipment and software, library resources, telephones, facsimile machines, photocopiers, office supplies, Internet connectivity, and access to Internet services and e-mail. Some examples of inappropriate personal uses of Government property, facilities, or services follow:

- (a) Accessing bulletin boards or other public forums without agency approval.
- (b) Installing and/or using any software unless authorized by management. This includes home use software (such as Real Player), screen savers, games, etc.
- (c) Developing a book for publication.
- (d) Developing appeals for altruistic causes without agency approval.
- (e) Using the equipment related to other employment or consulting for personal gain.
- (f) Sharing assigned computer ID and password with another user, or share with a user who is not authorized to have access to that application or program.
- (g) Creating or transmitting chain letters.
- (h) Creating/viewing/downloading of the following:
  - (1) Sexually explicit or sexually oriented materials.
  - (2) Gambling.
  - (3) Activities related to commercial or other non-government business purposes.
  - (4) Sites depicting, encouraging, or espousing the use of violence.
- (i) Use that could cause congestion, delay, degradation, or disruption of service to any government system or equipment.
- (j) Unauthorized acquisition, use, reproduction, transmission, and distribution of computer software or other material protected by copyright laws, trademark, or other property rights.

## National Information Security Handbook

**Compliance.** Any questions an employee may have regarding authorized or official use of equipment in an office should be directed to the employee's supervisor who may contact the Security Officer for answers. The agency reserves the right to remove from its information systems any material it views as offensive or potentially illegal. This includes information that may constitute sexual, ethnic, or racial harassment, including electronic mail, internal mail, and Internet access. Illegal information is strictly prohibited and is cause for disciplinary action which may include termination. Use of good judgment in complying with this policy will help prevent computer security problems and assure the protection of agency data. The agency shall protect the information we rely on to perform our duties. The first time an employee is found to be using government equipment for inappropriate use will result in a counseling session. Subsequent incidents of misuse may result in disciplinary action, such as denying the employee access to that equipment/system or in the removal of the employee from the agency.

**Privacy.** Employees, partners, and contractors who use USDA telecommunications do so with the understanding that such use serves as consent to monitor any type of use, including incidental and personal uses. NRCS may implement monitoring tools to detect improper use. Managers and supervisors are also authorized to access any electronic communication done using government equipment. NRCS has taken disciplinary action, up to and including removal, against employees found to be improperly using government equipment.

I hereby acknowledge that I have read the above privacy information and agree to comply with it and will access only authorized data.

---

Print User's Name

User's Signature & Date

Return this signed form to the IT staff for retention.

### 615.7 Exit Interview Questions

IT personnel must perform a Security Clearance Exit Interview when an employee leaves the office for any reason. Please contact the IT Manager to arrange a date and time.

Date of security clearance exit interview: \_\_\_\_/\_\_\_\_/\_\_\_\_

Name (Last, First, MI) \_\_\_\_\_

Staff: \_\_\_\_\_ Position Held \_\_\_\_\_

If leaving office or NRCS, new location: \_\_\_\_\_

Does the individual desire to take some files with him or her? (Y/N) \_\_\_\_

Will someone replace the individual leaving? (Y/N) \_\_\_\_

*If so*, will the replacement employee need access to these files? (Y/N) \_\_\_\_

During the interim period,

Who will need access to the individual's files? \_\_\_\_\_

Who will need access to the individual's electronic mail? \_\_\_\_\_

If the employee has a Government Calling Card, accountability will transfer with the employee. Notify the Administrative Staff or IT Manager to change the accountability. If the employee is leaving NRCS, the Government Calling Card must be returned to Administrative Staff or IT Manager.

FOR IT USE ONLY	
Login ID:	_____
Group Name(s):	_____
Home Directory:	_____
Alias Name(s):	_____

Transfer files to \_\_\_\_\_ on machine \_\_\_\_\_

If transferring, send files to new location by \_\_\_\_\_.

National Information Security Handbook

Individual Completing Request: \_\_\_\_\_

Date Completed: \_\_\_\_/\_\_\_\_/\_\_\_\_

IT staff will retain this form in accordance with the NRCS Records Guide.

National Information Security Handbook

615.8 Security Clearance Exit Interview

I, \_\_\_\_\_, have received a Natural Resources Conservation Service (NRCS) IT Security Debriefing. I certify that I have turned in all NRCS computer-related equipment, manuals, proprietary software, data, and NRCS “official use only” software or data. I will not disclose United States Department of Agriculture (USDA) sensitive/confidential information or Computer Center account numbers/passwords of which I became knowledgeable through my employment with NRCS. I understand that I am no longer authorized to access the USDA Computer Centers or any other computer facility under the authority of NRCS unless USDA or NRCS permission to do so is granted by the appropriate Federal officials.

\_\_\_\_\_  
(Signature) (Date)

\_\_\_\_\_  
(Witness) (Date)

IT staff will retain this form in accordance with NRCS Records Guide.

## 615.9 Federal Computer Incident Responses Capability (FedCIRC) Detail Report

The following is a reformat of the contents of the FedCIRC detail report. This information will meet the requirements for reporting a major incident.

### 1. General Information

- a. Incident Number or Code: \_\_\_\_\_
- b. Year: \_\_\_\_\_
- c. Agency Code: \_\_\_\_\_
- d. FedCIRC Incident Number \_\_\_\_\_
- e. Reporting Site Organization Name: \_\_\_\_\_
- g. Domain Name: \_\_\_\_\_
- h. Brief Description of the Affected Organization: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

### 2. Contact Information

- a. **Primary Contact:** \_\_\_\_\_
  - (1) E-mail Address: \_\_\_\_\_
  - (2) Telephone Number: \_\_\_\_\_
  - (3) Fax Number: \_\_\_\_\_
  - (4) Pager Number: \_\_\_\_\_
  - (5) Home Telephone Number: \_\_\_\_\_
  - (6) Secure Communication Channel (Yes/No): \_\_\_\_\_
- b. **Secondary Contact:** \_\_\_\_\_
  - (1) E-mail Address: \_\_\_\_\_  
\_\_\_\_\_

- (2) Telephone Number: \_\_\_\_\_  
\_\_\_\_\_
- (3) Fax Number: \_\_\_\_\_
- (4) Pager Number: \_\_\_\_\_
- (5) Home Telephone Number: \_\_\_\_\_
- (6) Secure Communication Channel (Yes/No): \_\_\_\_\_

**c. Security Officer Name::** \_\_\_\_\_

- (1) E-mail Address: \_\_\_\_\_
- (2) Telephone Number: \_\_\_\_\_
- (3) Fax Number: \_\_\_\_\_
- (4) Pager Number: \_\_\_\_\_
- (5) Home Telephone Number: \_\_\_\_\_
- (6) Secure Communication Channel (Yes/No): \_\_\_\_\_

**3. Contact from Other Site(s) Involved in this Incident:**

- a. Site Name: \_\_\_\_\_
- b. Contact Name: \_\_\_\_\_
- c. E-Mail Address: \_\_\_\_\_
- d. Phone Number: \_\_\_\_\_
- e. Pager Number: \_\_\_\_\_
- f. Fax Number: \_\_\_\_\_
- g. Secure Communication Channel (Yes/No): \_\_\_\_\_

**4. Information about Other USDA Contacts:**

- a. USDA Organization \_\_\_\_\_

b.	Organization Address:	_____
c.	Contact Name:	_____
d.	E-Mail Address:	_____
e.	Telephone Number	_____
g.	Fax Number:	_____

**5. Contact Information about Site through which Incident Occurred**

a.	Site Name:	_____
b.	Contact Name:	_____
c.	E-Mail Address:	_____
d.	Phone Number:	_____
f.	Pager Number:	_____
g.	Fax Number:	_____
h.	Secure Communication Channel (Yes/No):	_____

**6. Contact Information about Site from which Incident Began**

a.	Site Name:	_____
b.	Contact Name:	_____
c.	E-Mail Address:	_____
d.	Phone Number:	_____
e.	Pager Number:	_____
f.	Fax Number:	_____
g.	Secure Communication Channel (Yes/No):	_____
h.	Domain Name:	_____

**7. Contact Information about USDA ISSPM or OIG Contact(s)**

- a. Contact Name: \_\_\_\_\_
- b. E-Mail Address: \_\_\_\_\_
- c. Phone Number: \_\_\_\_\_
- d. Pager Number: \_\_\_\_\_
- e. Fax Number: \_\_\_\_\_

**8. Host Information: Please provide information about all host(s) involved in the incident. Each host shall be listed separately.**

- a. Host Name: \_\_\_\_\_
- b. IP Addresses: \_\_\_\_\_
- c. Vendor Hardware: \_\_\_\_\_
- d. Operating System and Version: \_\_\_\_\_

**9. Security patches applied/installed as currently recommended by the vendor. List version and date of installation. (Please provide on separate sheet of paper.)**

- a. Function(s) of the Involved Host: \_\_\_\_\_
- b. Router: \_\_\_\_\_
- c. Server: \_\_\_\_\_
- d. Mail Hub: \_\_\_\_\_
- e. DNS – External or Internal: \_\_\_\_\_
- f. Where on the Network is the Involved Host? Backbone, subnet: \_\_\_\_\_
- g. Nature of the Information at Risk on the Involved Host – \_\_\_\_\_

configuration, proprietary,  
personnel, financial, Privacy  
Act:

- h. Time Zone of the Involved Host: \_\_\_\_\_
- i. Were Clocks Synchronized? (Yes/No) \_\_\_\_\_
- j. Was the Host the Source or Victim of the Attack or Both? \_\_\_\_\_
- k. Was this Host Compromised as a Result of the Attack? (Yes/No) \_\_\_\_\_

**10. Incident Categories. All categories applicable to the incident shall be documented.**

- a. Probes(s): \_\_\_\_\_
- b. Scan(s): \_\_\_\_\_
- c. Prank: \_\_\_\_\_
- d. Scam: \_\_\_\_\_
- e. E-Mail Spoof: \_\_\_\_\_
- f. E-Mail Bombardment: \_\_\_\_\_
- g. Was this a denial-of-service attack? \_\_\_\_\_

**11. Break-In. In each of the following, indicate Yes or No.**

- a. Intruder gained "root access": \_\_\_\_\_
- b. Intruder installed a Trojan horse program: \_\_\_\_\_
- c. Intruder installed a packet sniffer: \_\_\_\_\_

packet sniffer:

- d. If Yes,
  - (1) What was full path name(s) of the sniffer output file(s) \_\_\_\_\_
  - (2) How many sessions did the sniffer log? Use "grep -c 'DATA'<filename>" to obtain this information) \_\_\_\_\_
- e. NIS (yellow pages) attack: \_\_\_\_\_
- f. NFS attack: \_\_\_\_\_
- g. TFTP attack: \_\_\_\_\_
- h. FTP attack: \_\_\_\_\_
- i. Telnet attack: \_\_\_\_\_
- j. rlogin or rsh attack: \_\_\_\_\_
- k. Cracked password: \_\_\_\_\_
- l. Easily-guessable password: \_\_\_\_\_
- m. Anonymous FTP abuse: \_\_\_\_\_
- n. IP Spoofing: \_\_\_\_\_
- o. Product vulnerability. Explain: \_\_\_\_\_
- p. Misuse of host(s) resources: \_\_\_\_\_

**12. Security Tools. At the time of the incident, was the organization using any of the following? (Yes/No)**

- a. Network Monitoring Tools: \_\_\_\_\_

- b. Authentication/Password Tools \_\_\_\_\_
- c. Service Filtering Tools: \_\_\_\_\_
- d. Tools to Scan Host for Vulnerabilities – ISS/SATAN: \_\_\_\_\_
- e. Multipurpose Tools: (Circle all that apply)
  - security
  - C COPS
  - Tiger
- f. Other Tools: (Circle all that apply)
  - Lsof
  - cpm
  - smrsh
  - append-only file systems
  - virus scanner(s)
- g. Were logs being maintained? If so, please describe \_\_\_\_\_

**13. Detail Incident Description. This should be as detailed as possible, especially when writing lessons learned or an after incident follow-up report. Please use separate sheets of paper to address the following.**

- a. Date and duration of incident
- b. How was the incident discovered
- c. Method(s) use by intruders to gain access to host(s)
- d. Detailed discussion of vulnerabilities exploited that are not addressed in

exploited that are not addressed in previous sections

- e. Hidden files/directories
- f. Source of attack (if known)
- g. How did/does your organization plan to address the incident
- h. Attach log file

**615.10 Annual IT Security Review and Risk Assessment**

**A. ANNUAL IT SECURITY REVIEW**

Office		Area Office	
Office Type		Date of Previous Review	
Address		City	
		State	

*NOTE:* The person preparing this plan is verifying that all areas have been assessed and analyzed for security risks and vulnerabilities.

Prepared By		Date	
Title		Telephone Number	
Agency			
Prepared By		Date	
Title		Telephone Number	
Agency			
Prepared By		Date	
Title _		Telephone Number	
Agency			

*NOTE:* The person reviewing this plan is verifying that all areas have been assessed and analyzed for security risks and vulnerabilities.

National Information Security Handbook

Reviewed by		Date	
Title		Telephone Number	
Agency			
Reviewed by		Date	
Title		Telephone Number	
Agency			
Reviewed by		Date	
Title		Telephone Number	
Agency			

This security review document has been designed to allow the three partner agencies to use for each office. The questionnaire will be completed in each office and forwarded to the next higher level for review.

National Information Security Handbook

<b>ADMINISTRATIVE CONTROLS</b>	<b>YES</b>	<b>NO</b>	<b>N/A</b>
List occupants of building other than Federal Government: _____ _____ _____			
Is there an Emergency Response Plan available for the office? If yes, date of plan _____	___	___	___
Does the plan include phone numbers for police and fire departments and agency security officer?	___	___	___
Is IT security assigned to agency individual(s)?	___	___	___
Are those individuals trained in security measures?	___	___	___
Have security policies, procedures, and standards been distributed to all employees in the office?	___	___	___
Compliance with security policies, procedures, and standards are regularly monitored?	___	___	___
Local policies and regulations have been distributed and are being followed?	___	___	___
<b>SECURITY AWARENESS AND TRAINING</b>			
Annual security training is offered to all office employees, partners, and contractors?	___	___	___
Formal	___	___	___
Brochures	___	___	___
Film	___	___	___
Other _____	___	___	___
Training on system usage is completed prior to granting computer and system access?	___	___	___
Training is provided on the procedures for reporting security problems or incidents (viruses, hackers, theft, etc.)?	___	___	___

National Information Security Handbook

<b>ADMINISTRATIVE CONTROLS</b>	<b>YES</b>	<b>NO</b>	<b>N/A</b>
problems or incidents (viruses, hackers, theft, etc.)?			
<b>PERSONNEL CONTROLS</b>			
Do employees, partners, and contractors have background screening and security investigations in accordance with National IRM Manual, Part 502)?	___	___	___
Are new employees and contractors given a briefing that explains their security responsibilities?	___	___	___
Are duties separated such that the person who authorizes a payment to a client does not issue the payment? (This pertains to FSA and RD employees.)	___	___	___
Are user IDs promptly suspended for terminated or transferring employees, partners, and contractors?	___	___	___
Are security-related identifications, cards, keys, etc., retrieved from individuals who depart from the agency or office?	___	___	___
Are the appropriate exit interview reports completed and forwarded to appropriate officials? (See Parts 615.4, 615.7 and 615.8.)	___	___	___
<b>PHYSICAL PROTECTION</b>			
Is access to the office controlled by protection systems? (Circle the appropriate system) Keys, Guards, Keycard System, Other _____	___	___	___
Are computer and telephone rooms located in an area that is restricted to authorized employees, partners, and contractors only?	___	___	___
Are restricted spaces locked when authorized users are not present?	___	___	___
Are escorts provided for visitors to restricted areas?	___	___	___
Is computer equipment secured and logged off at the end of the work day?	___	___	___
Are laptops secured when not in use?	___	___	___

National Information Security Handbook

<b>ADMINISTRATIVE CONTROLS</b>	<b>YES</b>	<b>NO</b>	<b>N/A</b>
Is an up-to-date inventory of all computer equipment and information resources maintained for the office?	___	___	___
Are office door keys controlled, and is distribution periodically verified?	___	___	___
Is a security log maintained for visitors and employees before and after office hours?	___	___	___
Are there procedures for checking physical security at the end of each day?	___	___	___
Are perimeter walls slab to slab in construction and permanently attached to true floor and true ceiling?	___	___	___
Do ground-level and second-story windows have positive locking devices installed?	___	___	___
Are doors to the computer and telecommunications facilities solid wood or metal at least 1-3/4 inches thick?	___	___	___
Are doors secured with deadbolt locks with a one-inch throw and a high-security cylinder (e.g., Medeco D-11 series)?	___	___	___
Are keys "off-master" in buildings shared with other entities?	___	___	___
Are cipher locks used to control access to computer facilities?	___	___	___
Are cipher combinations at least four numbers?	___	___	___
Are cipher combinations changed at least every six months or when anyone with the combination no longer requires access?	___	___	___
Do police or guards regularly patrol and check the building?	___	___	___
Emergency response time for:			
Police Department _____			
Fire Department _____			
Rescue Squad _____			
Are periodic fire and emergency evacuation drills conducted?	___	___	___

National Information Security Handbook

<b>ADMINISTRATIVE CONTROLS</b>	<b>YES</b>	<b>NO</b>	<b>N/A</b>
Are there fire detection and suppression systems in the office? If "yes," which type (circle appropriate system):	___	___	___
Smoke detectors and/or heat detectors			
General purpose fire extinguishers (Type ABC)			
Dry chemical (Type BC)			
Halon			
Sprinkler system			
Do fire detection and suppression systems automatically notify fire department as well as staff?	___	___	___
Are portable fire extinguishers checked annually?	___	___	___
Are employees trained in the use of fire extinguishers?	___	___	___
Is there emergency lighting in the office?	___	___	___
Are emergency computer equipment shut-down procedures documented and tested?	___	___	___
Are sensitive data and hard copy documents protected from unauthorized exposure and access?	___	___	___
Are there shredders in the office?	___	___	___
Are computers that process sensitive data protected from viewing by unauthorized individuals?	___	___	___
Are food and beverages kept away from computers?	___	___	___
Are physical sites safe from environmental threats?	___	___	___
Are critical computers and telecommunications equipment protected from power fluctuations with surge protectors?	___	___	___
Are areas around IT equipment free of obstructions and kept orderly?	___	___	___

National Information Security Handbook

<b>ADMINISTRATIVE CONTROLS</b>	<b>YES</b>	<b>NO</b>	<b>N/A</b>
<b>PBX OR TELEPHONE KEY SYSTEMS</b>			
Are PBXs and key systems protected in the same manner as servers?	___	___	___
Is this equipment password protected?	___	___	___
Is the password changed at least twice a year?	___	___	___
<b>SOFTWARE AND APPLICATION PROTECTION</b>			
Do nonsystem administration personnel have sysadmin or root passwords?	___	___	___
Have all default account passwords been changed or accounts removed?	___	___	___
Are unique logins and passwords required for system access?	___	___	___
Are user IDs and passwords held in strict confidence and safeguarded from unauthorized access, use, and disclosure?	___	___	___
Are users required to create passwords that contain at least eight characters that include at least three of the following – lower case, upper case, numbers, and special characters?	___	___	___
Are passwords changed periodically or when it is suspected that they might have been compromised?	___	___	___
Are sensitive data files password protected?	___	___	___
Do users log off or have a password-protected screen saver active when a personal computer is not in use after a short period of time?	___	___	___
Are updated antivirus checking programs on all personal computers and laptops and being used?	___	___	___
Do users know the precautions to take to prevent a computer from being infected with a virus?	___	___	___
Are software copyright and licensing agreements adhered to?	___	___	___
Are audit logs reviewed to track system access and problems that occur?	___	___	___

National Information Security Handbook

<b>ADMINISTRATIVE CONTROLS</b>	<b>YES</b>	<b>NO</b>	<b>N/A</b>
occur?			
Is access to information and systems granted based on “need to know” to perform only official Government business?	___	___	___
Do dial-up connections required user identification and password?	___	___	___
Is there dial up access to or from the office?	___	___	___
<b>SECURITY PLANNING</b>			
Is there a security plan, contingency plan, and risk assessment completed?	___	___	___
Are documents readily available for use in case of an emergency?	___	___	___
Is the contingency plan documented, reviewed, and tested periodically?	___	___	___
Has the contingency plan been tested within the past year?	___	___	___
Are these documents updated annually or when a major change occurs?	___	___	___
Have these documents been forwarded to the next level of responsibility?	___	___	___
Are data, software, applications and information backed up regularly?	___	___	___
If “Yes,” address and phone number of offsite location: _____ _____			
Frequency and type of backups (e.g., incremental, full) and number of rotations retained: _____ _____			

National Information Security Handbook

<b>ADMINISTRATIVE CONTROLS</b>	<b>YES</b>	<b>NO</b>	<b>N/A</b>
Is there a fireproof safe in office or offsite locations that is used for storage of backup tapes?	___	___	___
Are storage media properly identified as to their content and information sensitivity?	___	___	___
Are the procedures in the Common Computing Environment system administrator and user guides followed ?	___	___	___
Are specific responsibilities identified and assigned for system recovery procedures?	___	___	___
Are critical applications identified, documented, and backed up on a regular basis?	___	___	___
Are configurations and documentation for computers and information resources periodically reviewed and updated?	___	___	___
Have backup tapes been tested to ensure integrity and readability? If "yes," date of last test: _____	___	___	___
Have any break ins, computer viruses, incidents, or violations been detected during the year?	___	___	___
If "yes," specify the date of the incident and list actions taken: _____ _____ _____ _____ _____ _____			

*NOTE:* For questions with "NO" as a response and do not meet the definition of "low risk", provide an explanation of how the risk will be mitigated.