

National Information Security Handbook

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;

National Information Security Handbook

- (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.