

1. CHAPTER ONE: ACCEPTABLE USE SECURITY POLICY

a. General Policy Statement

This policy establishes the acceptable use of USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) information systems that support the Service Center Agencies (SCA) including Large Offices, Field Offices, and their partners. This includes the use of information systems, Internet access, and electronic mail (e-mail). OCIO-ITS information systems provide critical support to the Service Center Agencies. Using OCIO-ITS information resources for inappropriate, unauthorized, or unlawful activities can seriously undermine the ability to accomplish the organizational function. Users shall make every effort to employ OCIO-ITS information resources in an appropriate and acceptable manner, according to the guidelines defined in this policy.

b. Policy Detail

(1). Official Business

- (a). The OCIO-ITS provides information resources to the Service Center Agencies for the purpose of transacting official business. Official business may be defined as any information processing that is required to perform associated work responsibilities.
- (b). Official business includes, but is not limited to, the performance of OCIO-ITS work-related duties in position descriptions, professional training, and tasks directed via contracts and support activities related to contract tasking. However, USDA DR 3300-1 authorizes limited personal use provided this use involves minimal expense to the Government and does not interfere with official business.

(2). Rules of Behavior

Rules of behavior guidelines for the use of OCIO-ITS information systems include, but are not limited to, the following:

- (a). Users shall protect their UserIDs and passwords from disclosure in accordance with Chapter 3: Authorization and Access Control Security Policy or its replacement.
- (b). Participants shall ensure that password resets are performed securely in accordance with Chapter 3: Authorization and Access Control Security Policy or its replacement.
- (c). Users shall change their password if compromised, i.e., someone else knows their password. Users shall immediately notify their supervisor or security administrator for all suspected or confirmed password compromises. Passwords will be changed in accordance with Chapter 3: Authorization and Access Control Security Policy or its replacement.
- (d). Participants shall not program their login or password into automatic script routines or programs in accordance with Chapter 3: Authorization and Access Control Security Policy or its replacement.
- (e). Users shall log off, sign off, or lock the computer system when going to lunch or a break, or any time they leave their computer or terminal.
- (f). Participants shall retrieve all hard-copy printouts in a timely manner. If the originator or receiver of a printout cannot be determined, dispose of it accordingly.

- (g). Users shall inform their supervisor about all sensitive applications or data that will be placed on a system and on any equipment processing sensitive information, so that appropriate security measures can be implemented.
- (h). Participants must not use OCIO-ITS computers or licensed software for personal use beyond those set by the limited personal use policy.
- (i). Users shall not use personal equipment or software for official business without their supervisor's written approval; sensitive information is not permitted on personal computers.
- (j). Participants will not install or use unauthorized software on OCIO-ITS equipment to include the use of freeware, shareware, or public-domain software without their supervisor's permission and without scanning it for viruses.
- (k). Participants shall comply with local office policy on the use of antivirus software in accordance with Chapter 27: Virus Protection Security Policy or its replacement.
- (l). Users shall observe all software license agreements and will not violate federal copyright laws.
- (m). Participants will not move equipment or exchange system components without their manager's or supervisor's approval.
- (n). OCIO-ITS computer equipment shall be physically protected from hazards such as liquids, food, staples, and paper clips. Refer to Chapter 17: Physical Access Security Policy, or its replacement, for additional information.
- (o). Users shall properly protect and label magnetic media in accordance with Chapter 7: Data Management Security Policy or its replacement.
- (p). Participants must not disclose any dial-in telephone numbers or procedures that permit system access from a remote location. Refer to Chapter 14: Network Access Security Policy, or its replacement, for additional information.
- (q). Users shall not disclose or discuss any OCIO-ITS information, whether sensitive or non-sensitive, with unauthorized individuals. The Privacy Act of 1974, 5 U.S.C. 552a, prohibits such disclosure. Refer to Chapter 11: Information Classification Security Policy, or its replacement, for additional information.
- (r). Participants shall be cognizant of the nature of security incidents and must promptly report them to their supervisor in accordance with Chapter 11: Incident Identification, Declaration, Reporting, and Handling Security Policy or its replacement. Examples include, but are not limited to, unauthorized disclosure of information, computer viruses, theft of equipment, software, or information, inappropriate use, and deliberate alteration or destruction of data or equipment.

(3). Personal Use

- (a). Appropriate Use
Limited personal use of OCIO-ITS information systems is permitted if it is determined that such communication:
 1. Does not adversely affect the performance of official duties
 2. Are of reasonable duration and frequency
 3. Serve a legitimate public interest, such as researching and gathering information from other U.S. Government Agency websites or partner websites.
 4. Does not put Federal Government telecommunication systems to uses that would reflect adversely on the OCIO-ITS, to include activities that are

illegal, inappropriate, or offensive to fellow employees, partners, contractors or the public.

(b). Inappropriate Use

Inappropriate personal use of OCIO-ITS information systems include, but are not limited to:

1. Any personal use that could cause congestion, delay, or disruption of service to any Government system or equipment, to include:
 - a. Use of any personal remote access device while connected to any OCIO-ITS LAN to include the use of modems, cellular modems, PDAs, etc.
 - b. Playing online electronic games
 - c. Use of "Push" technology on the Internet and other continuous data streams, i.e., streaming video/music/radio broadcasts, and ticker tape banners such as stock quotes, weather, etc., that would degrade the performance of the entire network
 - d. Creating, copying, transmitting, or retranslating chain letters or other unauthorized mass mailings
 - e. Use of instant messaging to include AOL Instant Messenger, Yahoo Instant Messenger, ICQ, Microsoft, etc.
 - f. Use of peer-to-peer file sharing applications such as Gnutella, KaZaA, Musiccity.com, BearShare, LimeWire, XoloX, Auto galaxy, Direct Connect, ToadNoad, WinMx, Napigator, Morpheus, CuteMx, Scour Exchange, FreeNetfile, eDonkey, and iMesh
2. Activities that are illegal, inappropriate, or offensive to fellow employees, partners, contractors or the public
3. Creating, downloading, viewing, storing, copying, or transmitting; sexually explicit or sexually oriented materials, material related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities otherwise prohibited
4. Use of OCIO-ITS information systems for commercial profit-making activities in support of other outside employment or business activities
5. Engaging in any outside fundraising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity
6. Use for posting OCIO-ITS information to external newsgroups, bulletin boards, or other public forums without authority
7. The unauthorized acquisition, use, reproduction, transmission, and distribution of computer software or other material protected by national or international copyright laws, trademarks, or other intellectual property rights
8. Representing one's self as someone else
9. Soliciting Government employees or providing information about or lists of OCIO-ITS employees to others outside the Government without authorization
10. Interfering with the employee's job, the jobs of other employees, or the operation of the Internet gateways
11. Any type of personal solicitation
12. Modifying Government office equipment for non-Government purposes, including loading personal software or making configuration changes

13. Intentionally or negligently causing the propagation of viruses, Trojan horses, or other malicious software

(4). E-Mail Use

(a). Appropriate E-Mail Use

Appropriate e-mail use includes, but is not limited to:

1. Limited personal use of the OCIO-ITS e-mail system during an employee's non-work time, such as break times and lunch periods
2. Any message containing information exchanged by employees for the purpose of accomplishing government business
3. Use of the OCIO-ITS e-mail system by authorized users that does not interfere with official business nor reflect adversely on the OCIO-ITS
4. E-mail message forwarding or some other method shall be employed when an addressee is unavailable to receive mail that is required to move business processes
5. The use of Notepad to open e-mail attached files ending with the extensions .vb, .vbe, .vbs, .wsc, .wsh, .wsf, .pif, .scr, .reg, .js, and jse to limit the spread of various VBScript viruses and worms
6. Access to the OCIO-ITS e-mail system by users when they are not at their duty station site, or at another installed site, shall only occur through the secured OCIO-ITS dial-up or VPN access points
7. Transmitting sensitive information that is encrypted and password protected to include, but not limited to, the following:
 - a. Proprietary USDA and OCIO-ITS information
 - b. U.S. Government credit card numbers
 - c. Designated For Official Use Only (FOUO), Sensitive But Unclassified (SBU), or Sensitive Security Information (SSI) information
 - d. Risk assessments, audit findings, or any other documentation containing known OCIO-ITS information system vulnerabilities
 - e. Privacy Act data
 - f. OCIO-ITS network access information to include, but not limited to, IP addresses and local/remote workstation IP addresses, port numbers, dial-in access numbers, or associated system passwords used for gaining entry to networks

(b). Inappropriate E-Mail Use

1. Inappropriate e-mail use includes, but is not limited to:
 - a. Sharing a UserID and password to obtain access to another user's mail for any purpose
 - b. Opening attached file extensions on OCIO-ITS e-mail servers to include .ade, .adp, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .exe, .hta, .ins, .isp, .lnk, .mda, .mde, .mdz, mp3, .msc, .msi, .msp, .mst, ocx, .pcd, .pif, .reg, .sct, and .shs
 - c. Using a personal Internet Service Provider (ISP) to gain access to the OCIO-ITS e-mail system or for any other system operation or service
 - d. Using wireless service providers outside of OCIO-ITS approved Federal facilities is forbidden
 - e. Transmission of any unencrypted and non-password protected sensitive information

2. E-mail privileges will be removed immediately if other than acceptable or appropriate use is discovered.

(5). Internet Use

- (a). Appropriate Internet use includes, but is not limited to:
 1. Limited personal use of the Internet during an employee's non-worktime
 2. 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
 3. Development of Internet Web-based projects as established by business need
 4. Sharing of information without compromising OCIO-ITS secured data
 5. Exchange of any inter-Agency non-sensitive data in support of departmental mission, OCIO-ITS missions, or other official purposes
 6. Distribution and collection of information related to official program delivery.
 7. Transmitting U.S. Government credit card numbers for legitimate official business, i.e., booking air, car, or hotel information at a secured website for purposes of official Government travel

- (b). Inappropriate Internet Use
Inappropriate Internet use includes, but is not limited to:
 1. Purposely visiting adult entertainment, pornographic, and gambling websites
 2. Downloading, copying, sharing, or sending software, music videos, movies, or pictures (whether purchased or not purchased) that are not job related as use of these constitutes copyright violations and is a non-business use of limited network bandwidth
 3. Peer-to-peer software and file sharing products not expressly identified for authorized use may not be used on or through OCIO-ITS servers and workstations
 4. Subscribing to 'list servers', 'use groups', or 'bulletin boards' that do not align to authorized business needs
 5. Personal use of streaming video, music and radio consumes bandwidth could cause congestion, delay, or disruption of service due to bandwidth constraints