



# Security Incident Response Guide For Users

---

## USDA Service Center Agencies

- Farm Service Agency (FSA)
- Natural Resources Conservation Service (NRCS)
- Rural Development (RD)

## OCIO-Information Technology Services

---

### *I. What Is A Security Incident?*

- ✓ Any event that violates laws, regulations or security policies.
- ✓ Loss of control of your PC. If anything happens that you did not make happen, other than automatic updates (which usually happen during off-hours).
- ✓ Employee abuse, that includes: pornography, peer-to-peer file sharing, unauthorized software installation and other actions that violate the acceptable use policy.
- ✓ Attempts by unauthorized people to obtain access (physical or electronic) or sensitive information, for example by phone, e-mail, or in person. (Social Engineering)
- ✓ Attempts by unidentified or unauthorized people to obtain sensitive personal or business information through deceptive means, such as fraudulent but official-looking e-mails. (Phishing)
- ✓ Sensitive official government materials found unsecured.



*Incidents are not limited to the above examples. Anything that seems as though it may be a violation should be reported.*

## ***II. Minimizing the Risk of E-Mail Based Incidents***

- ✓ Limit who sends e-mail to your account by asking friends, family members and non-business associates to not send e-mail messages to your government e-mail address.
- ✓ Do not open an attachment in your e-mail if you do not know the person who sent it or if you are not familiar or comfortable with the extension for the attachment. Viruses may be embedded in the attachment, such as an attachment with the extension .exe, .pif, .com, .zip, etc. An infected file will often execute as soon as it is opened. Report any suspicious e-mails with or without attachments.
- ✓ If you have opened an attachment by mistake, contact your supervisor and the ITS Service Desk immediately.
- ✓ If you receive material via e-mail that is inappropriate, such as pornographic or offensive material, notify your supervisor immediately. Incidents of this nature will need to be reported to your agency Information Systems Security Office.
- ✓ Avoid looking at personal, web-based e-mail accounts such as Yahoo, Gmail, or Hotmail while on the office network.

## ***III. Avoiding Internet-Based Incidents***

- ✓ Avoid websites with questionable content, established by [acceptable use policy](#) and avoid abusive behavior.
- ✓ Do not accept downloads that are unsolicited. When in doubt, always click “Cancel” or close the window.
- ✓ Refrain from visiting or communicating in Internet-based “chat” rooms. Do not participate in Peer-to-Peer file sharing such as Kazaa or Limewire, etc.
- ✓ Limit the amount of time you spend “surfing” the Internet.

## ***IV. Use of Personal Equipment***

- ✓ Make sure a virus scan is performed on all portable media and disks (floppies, CDs, thumb drives, etc) that you bring in prior to connecting them, or inserting them in, to your PC. If you need assistance, please call the ITS Service Desk.
- ✓ Personal laptop computers and portable devices are not allowed on the network, unless you have explicit authorization from your supervisor. The OCIO-ITS Vulnerability Scan Security Procedures Guide states all non-USDA equipment must pass a complete vulnerability scan before allowed connection to the network.

*All personal equipment, once connected to the network, will be subject to USDA and agency policies and network monitoring.*

## ***V. Common Symptoms of an Incident***

- ✓ Your PC seems to perform slower than usual.
- ✓ Your screen occasionally flashes for no apparent reason.
- ✓ Your PC often reboots, crashes, locks up or does not respond to your commands.
- ✓ New programs that you do not recognize have been installed.
- ✓ Frequent appearance of “pop-up” windows.

## ***VI. Who To Contact About Incidents***

- ✓ For any suspected employee misuse of IT equipment (including pornographic and illegal activities), immediately contact the Information Systems Security Program Manager (ISSPM) of the agency for which the suspected abuser works:  
ITS – 202-720-8650                      FSA – 202-720-2419  
NRCS/CD – 301-504-2242              RD – 314-335-8829
- ✓ All users are required to report all other incidents to their IT Service Desk
  - Large Office users call 800-457-3642  
  
(Fort Collins, St. Louis, Kansas City, Portland, Lincoln, Fort Worth, Salt Lake City, Washington Metro Area, Greensboro)
  - District, State, and County users contact your State IT Service Desk
  - Magic Self Service: <https://merlin.sc.egov.usda.gov/magicsshd/>

***WARNING:*** Violation of any provision of OCIO-ITS security policies may result in disciplinary action in accordance with USDA policy and the policies of the sponsoring agency. These actions can include: access limitations, restitution for improper use, initiation of legal action, and disciplinary action up to and including termination of employment.

*Provided by OCIO-ITS revised 5/25/2005*

# Common Terms and Definitions of Incidents

**Trojan Horse** - a malicious program disguised as legitimate software or is deliberately attached to otherwise useful software by a programmer.

**Virus** - a type of program that can replicate itself by making (possibly modified) copies of itself. The main criterion for classifying a piece of executable code as a virus is that it spreads itself by means of 'hosts' (PCs).

**Worm** - a self-replicating computer program, similar to a computer virus. However, a worm is self-contained and does not need to be part of another program to propagate itself.

**Social Engineering** - the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick a person into revealing sensitive information or getting them to do something that is against typical policies.

**“Phishing”** - the act of attempting to fraudulently acquire through deception sensitive personal information such as passwords and credit card details. This is accomplished by masquerading in an official-looking e-mail, IM, etc. as someone trustworthy with a real need for such information.

**Spamming** - the use of any electronic communications medium to send unsolicited messages in bulk, indiscriminately -- unlike sending to a selected group in normal marketing. In the popular eye, the most common form of spam is that delivered in e-mail as a form of commercial advertising.

**Malware** - (a portmanteau of "malicious software") is any software program developed for the purpose of causing harm to a computer system, similar to a virus or Trojan horse.

**Spyware** - consists of computer software that gathers and reports information about a computer user without the user's knowledge or consent.

**Adware** - any software application in which advertisements are displayed while the program is running. These applications include additional code that displays the ads in pop-up windows or through a bar that appears on a computer screen.

**Backdoor** - software that allows access to the computer system bypassing the normal authentication procedures.

**Exploit** - software that attacks particular security vulnerabilities. Exploits are not necessarily malicious in intent — they are often devised by security researchers as a way of demonstrating that vulnerabilities exist.