

Use of IT Systems

Table of Contents

| | |
|---|----------|
| Relevance to Security | 1 |
| Potentially Disqualifying Conditions | 2 |
| Judging Seriousness | 3 |
| Specific Online Behaviors of Concern | 4 |
| Sexually Explicit Material & Internet Abuse | 7 |
| Viruses | 7 |
| Security of Hard Drives | 8 |
| Mitigating Conditions | 9 |
| Unusual Circumstances | 9 |
| Organizational Efficiency | 9 |
| Misuse was Unintentional or Inadvertent | 10 |

Relevance to Security

Failure to comply with rules, procedures, guidelines or regulations regarding information technology (IT) systems raises concerns about an individual's reliability and trustworthiness, and calls into question the person's willingness or ability to properly protect sensitive systems, networks, and information. Such behavior is sometimes part of a more general pattern of inability or unwillingness to follow rules that should also be evaluated under the Personal Conduct guideline.

The term information technology systems as used here includes all computer hardware, software, firmware, networks, and data used for the communication, transmission, processing, manipulation, storage, or protection of information. While not always illegal, misuse of information technology systems is often unethical and usually reflects poor judgment or lack of care in following security rules and regulations.

As we store more and more information in computer databases, and as these databases become more closely linked in networks, more people have broader access to more classified and other sensitive information than ever before. This magnifies the amount of damage that can be caused by a single cleared insider working for the other side. As Senator Jay Rockefeller, Vice Chairman of the U.S. Senate Select Committee on Intelligence, put it: "A single spy today can remove more information on a disk than spies of yesteryear could remove with a truck." [1](#)

As it becomes easier for people to access computer databases, ease of use means ease of abuse. Using the computer, individual employees can quickly and quietly commit serious crimes that are very difficult to detect. They can

steal information, change information, or destroy information in automated file systems while sitting at their desk and doing nothing that appears out of the ordinary to casual observers.

Personnel with technical skills and administrative access to a network are also capable of damaging or impairing the operability of critical information systems. There have been numerous cases of such malicious behavior by disgruntled IT professionals with some level of administrative access to a government or corporate system. [2](#)

Owing to the magnitude of problems that can be caused by misuse of computer systems, all agencies have a vested interest in maintaining a work environment that fosters high standards of computer security. The work environment that tacitly ignores or tolerates petty violations is also the climate where serious violations are most likely to occur. [3](#)

Potentially Disqualifying Conditions

Extract from the Guideline

(a) illegal or unauthorized entry into any information technology system or component thereof;

(b) illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system;

(c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;

(d) downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system;

(e) unauthorized use of a government or other information technology system;

(f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations;

(g) negligence or lax security habits in handling information technology that persist despite counseling by management;

(h) any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

Employees who misuse information technology systems range widely from good people with bad security habits to bad people who commit serious crimes. Types of misuse range widely from accidental or careless security violations to ethical violations to sabotage and espionage. There is some overlap between the list of potentially disqualifying conditions under this guideline and under the Handling of Protected Information guideline.

Judging Seriousness

Factors that determine the security significance of the misuse of IT systems include the following:

- Whether the subject knew the behavior was against the rules but did it anyway.
- The intent of the behavior and the degree of malice. If the misuse was intentional, was it motivated by simple curiosity, the intellectual challenge of breaking into or manipulating a protected system, personal gain without intent to harm others, personal gain knowing it would harm other individuals or the organization, or an intentional effort to harm other individuals or the organization?
- The significance of the potential or actual harm.
- Whether the subject had received appropriate security awareness training related to information assurance and IT systems security. Very often security violations result from ignorance of policies and technical vulnerabilities.
- What the behavior tells us about an individual's attitudes toward rules and policies and the likelihood of further problems with that individual.

Systems administrators, programmers, and other IT professionals who hold positions of special responsibility are able to do significant damage. As a result, they should be held to a higher standard of computer security and ethical behavior.

Several behaviors are of particular concern when assessing individuals who have misused an information system. Any of the following suggest that IT misuse may reflect a pattern of behavior that is much more significant than any single offense.

- The misuse is part of a general tendency toward ignoring rules, irresponsible behavior, or indifference toward security.
- The misuse is part of a history of vindictive behavior. Computer systems offer a readily available vehicle as well as a target for expressing resentment, spite, anger, or hate by persons who perceive themselves as victims of an unjust supervisor or an uncaring government or corporate bureaucracy.

- The system is misused to enhance one's self-esteem by outsmarting others. Some computer buffs break into protected or compartmented systems just for the personal satisfaction of showing that they can do it. Misuse of information technology systems is seen as a game -- an intellectual challenge that one must win by demonstrating cleverness or superior knowledge. This attitude can be dangerous and may portend future misuse.

Specific Online Behaviors of Concern

Misuse that may warrant some form of adjudicative action commonly falls under one of the following categories. Many of these examples can also be adjudicated under other guidelines such as Personal Conduct, Mishandling Protected Information, Criminal Conduct, or Psychological Conditions.

Unauthorized Access

- Any illegal or unauthorized entry into any information technology system, whether motivated by curiosity or simply by the challenge of penetrating the system. This includes exceeding one's level of authorized access within a system or unauthorized intrusion into another government or company system by evading access controls.
- Any unauthorized monitoring of electronic communications or system services.
- Systematic browsing of files that are beyond one's need-to-know. Some evidence suggests that browsing is often a precursor to criminality.⁴ It can be analogous to a burglar casing a target to see how vulnerable it is. If the person doing the browsing sees an opportunity to steal valuable information with little chance of detection, it can greatly increase any temptation to engage in theft.
- Malicious use of another person's computer terminal without authorization when that person leaves the terminal unattended.

Modification, Destruction or Manipulation

- Any illegal or unauthorized modification or destruction of application software, files or records in an information technology system. This includes sabotaging or manipulating personnel records, research results, design specifications, etc. For example, two employees at a DoD medical laboratory changed drug test results in the computer system to show positive results as negative. Their purpose was not to help people get around the drug screening, but to reduce their own workload. Positive tests required additional work.
- Deliberately creating or allowing any unauthorized entry point or other system vulnerability in an information technology system.

- Denial of service, or disrupting a web site in a manner that renders it unusable to internal or external users. For example, in 1999 an Army Private First Class, who had been given a nonjudicial punishment for storing game files on a critical Army system, shut off access to the system by other personnel for over three hours. Given a second punishment, the same individual later deleted over 1,000 work-related files on the system by introducing a Trojan virus that allowed him to remotely control the workstations of other employees. The final offense resulted in a court martial and prison sentence. [2](#)

Use of IT System for Fraud, Theft, or Personal Gain

- Selling or otherwise exploiting for personal advantage classified, proprietary, Privacy Act, or other protected information.
- Manipulating financial records so that, for example, checks or money transfers are made out or sent to the wrong person.
- Manipulating logistics records to steal equipment. For example, equipment may be stolen by having it shipped to the wrong location. Thefts of equipment may be covered up by manipulating inventory records.
- Theft or illegal use of credit card numbers, altering of telephone billing accounts, cellular telephone billing numbers or any other communications fraud. As telephone systems are increasingly managed by computer, and as new technology merges all telecommunications, data transmission, cable television and teleconferencing, fraudulent use of these systems has increased. In a recent case, a foreign national employed by the U.S. Army at an overseas location altered phone records on line to make unlimited free phone calls.

Introduction of Unauthorized Software

- Installing, downloading, or using any unauthorized software or computer files, particularly without the use of an approved virus protection program.
- Inserting viruses and other malicious software (worms, Trojan Horses, logic bombs, trap doors) to destroy records or to penetrate or impair system functions. See [Viruses](#) for further information.
- The downloading, introduction, or use of hacking tools and the use of an information system to illegally enter other government or private sector systems or networks. In 1998 an Air Force enlisted man installed software on several office computers that allowed him to control them from his home personal computer. These intrusions and their source were detected by the AF Communication Emergency Response Team (AFCERT). A search of his personal computer

revealed evidence of hacking, software piracy, and the possession of child pornography. [5](#)

Misuse of Government or Corporate IT Systems

- Sending or soliciting sexually oriented messages or images. Downloading, creating, storing or displaying computer files of a sexual nature. See [Sexually Explicit Material](#) for additional information.
- Use of official equipment or systems to further an individual's private business enterprise. Apparently with no intention to harm the government system, in 1998 four enlisted service members set up their own local area network and a nongovernment commercial web site on a government server for the purpose of conducting a personal computer business after duty hours. While not a malicious act, this misuse of a military network may have compromised the network's capacity for meeting official requirements. [6](#)

Personal Harassment

- Transmission of offensive or harassing statements, including disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religious or political beliefs. Internet and e-mail access may make harassment easier because of its impersonal nature. Perpetrators need not be face-to-face with or engage in any truly personal contact with their victims. According to one report, the frequency of harassment has increased significantly as the use of local area networks and the Internet has increased. [7](#)
- Sexual harassment in the workplace using an IT system including solicitation, sexually explicit comments, obscene jokes, or other inappropriate communications sent by e-mail to a coworker with the intent to exploit, seduce, humiliate, embarrass or compromise that individual.

Failure to Protect Information

- Negligence or lax security habits in handling information technology that persist despite counseling by management. Examples of negligence include failure to protect a password and failure to promptly install software patches or updates as required. For possible mitigation of failure to protect a password, see [Organizational Efficiency](#) below.
- Removing electronic media containing classified information from the office to work on them at home.
- Processing classified information on a home PC or any other computer kept in an area that is not approved for secure storage, or moving a computer that has been used for classified material from a secure

area to a nonsecure area. (Classified files can be recovered on the hard drive even after they have been deleted or erased by the user.)

Sexually Explicit Material & Internet Abuse

One defense contractor that reviewed its Internet transactions found that 2% of all transactions were to sexually oriented sites. Almost 7% appeared to be to nonbusiness-related sites. A more recent survey of 305 Internet-enabled employees found that, in 2003, 2% of employees regularly accessed pornographic web content while at work.⁷ A large portion of the web content is pornographic in nature, with approximately 260 new pornographic web sites being launched each day.⁸

In a recent case involving a U.S. civilian employed by the Army overseas, child pornography was discovered on a classified government system during the course of a security investigation. The subject had used government laptops that contained classified information to link to the Internet to download the child pornography.⁹

Cyberporn addiction can be extremely costly for individuals and for the workplace. For more information see the sections on *Compulsive or Addictive Sexual Behavior* and *Sexual Addiction and the Internet* in the [Psychological Conditions](#) module.

Viruses

A virus is a very small, self-contained piece of computer code that is hidden within another computer program. Like a real virus, it can reproduce, infect others, and then lie dormant for months or years before it strikes. Whenever an infected computer interacts with another computer, the virus automatically reproduces itself in the other computer. In this way, a virus can spread quickly around the world. A computer worm spreads like a virus but is an independent program rather than hidden inside another program.

In a 2003 survey of 530 businesses, 82% reported viruses had been introduced into their business computers during the previous twelve months.¹⁰ In 2003, ICSA Labs 8th Annual Computer Virus Prevalence Survey reported a virus infection rate of over 100 virus detections per month per 1000 PCs surveyed. This number has increased annually for the past six years.¹¹

Over 80% of companies surveyed by ICSA reported a virus disaster (a case in which at least 25 computers were infected with a single virus at the same time) since June 2001. Of these, 75% reported lost productivity, 62% had corrupted files, 49% lost access to data, and 47% reported losing important data. The costs of these disasters vary. Based on their most recent disaster, the companies surveyed reported between 0 and 300 lost work days and

between \$2500 to over \$1,000,000 in financial losses. Median losses were four work days and \$10,000. [11](#)

Employees may unknowingly introduce a virus into a government or company network by bringing virus-contaminated software or games to the office and using them in office computers. Most viruses in the last few years, however, have been unknowingly downloaded as attachments to e-mails and are designed to automatically send the virus to every person in the victim's e-mail address book once the attachment is opened.

Many viruses are high-tech pranks not intended to cause damage. They may be designed, for example, to flash a certain message at a prescribed time on all of a network's computers. Others are intended to cause serious damage. Triggered by a predetermined event or date, the virus may tell a computer to delete files and application code or to disable all the computers in a network.

A computer programmer at a Fort Worth, Texas, insurance firm was convicted of computer sabotage for planting a virus that wiped out 168,000 payroll records two days after he was fired.

A computer programmer at defense contractor General Dynamics was arrested for planting a "logic bomb" set to go off several months after he resigned from the company. A logic bomb is a type of virus intended to destroy information at a specific time but not necessarily to spread from one computer to another. If the bomb had not been detected by another General Dynamics employee, it would have destroyed irreplaceable data on several defense contracts. [12](#)

Security of Hard Drives

Secrets in computers require the same level of protection as secrets on paper. Information can often be recovered from a computer hard drive even after the file has been deleted or erased by the computer user. As a result:

- Processing of classified information can be done only on systems that have been approved for that use.
- Storage devices, including hard drives, on which classified information has been prepared, must be kept in a secure area.
- When processing classified information on an approved computer in a nonsecure environment, it is necessary to use a removable hard drive that is secured in a classified container when not in use.
- A special program that wipes a hard disk clean should be used before moving a computer from a secure area to a nonsecure area or before disposing of the computer as excess equipment.
- Information systems authorized for the processing of classified information cannot be linked by phone or Internet to any external

unclassified system. Electronic media (CDs, flash drives, diskettes) used in classified systems must be appropriately marked and not used subsequently in an unclassified system.

- Storage devices and components of systems used for the processing of classified or sensitive information should not be sent to property disposal until a complete inspection confirms that its storage devices contain no retrievable information.

In two well-publicized cases, regional Department of Justice offices sold surplus computer equipment that had not been wiped clean. The hard disks contained information that could compromise confidential informants. [13](#)

Mitigating Conditions

Extract from the Guideline

(a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(b) the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available;

(c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.

The mitigating conditions are described in somewhat greater detail below.

Unusual Circumstances

Because it is difficult to foresee all the circumstances under which misuse of an information system may occur, there is also a general mitigating condition. Misuse may be mitigated if substantial time has elapsed since the misuse occurred, or it happened under such unusual circumstances that it is unlikely to recur and does not cast doubt on the subject's reliability, trustworthiness, or good judgment. The key element of this condition is not the amount of time that has elapsed, but an informed judgment that such behavior or other unreliable or untrustworthy behavior is unlikely to recur.

Organizational Efficiency

Misuse can be mitigated if it was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available. For example, an individual going away on vacation or a temporary duty assignment might ask a coworker to check his or her e-mail during this period. In some organizations, it takes several weeks before a new employee gets approval and a password for logging into the office network. During this period, the new employee's supervisor or a coworker might share their password with the new employee so that he or she can start working. This would be a violation of computer security rules, but done for a well-intentioned reason. If the subject of investigation claims that this or any other inappropriate activity was authorized by a supervisor, the investigator is supposed to corroborate this with the individual who reportedly authorized it.

Misuse was Unintentional or Inadvertent

Misuse can be mitigated if it was unintentional or inadvertent, especially if it was followed by a prompt, good-faith effort to correct the situation and the subject immediately notified his or her supervisor. Many people are still learning about the security requirements and potential risks associated with changes in computer technology and the rapid expansion of interrelated computer networks. They may not be aware that they cannot fully erase classified records from a hard disk. They may be unaware of the risk of spreading viruses through use of unauthorized disks or CD-ROMs. They may be unaware of copyright, licensing, or privacy issues. In this environment, unintentional or inadvertent misuse that results from lack of training may be the most frequent mitigating condition.

When caught violating the rules, some individuals claim to have been unaware of the rules. Investigators are supposed to report any information that supports or refutes such a claim, including the date and subject matter of any security awareness briefing or training when the relevant rule was covered.

Footnotes

1. Rockefeller, Sen. J. (2003). Speech urging the Senate to pass the Intelligence Authorization Act for Fiscal Year 2004. *Congressional Record: November 21, 2003 (Senate)*, pp. S15335-S15358.
2. Shaw, E.D., & Fischer, L.F. (2005) *Ten tales of betrayal: The threat to corporate infrastructures by information technology insiders* (TR 05-13). Monterey, CA: Defense Personnel Security Research Center.
3. Hollinger, R.C. (1989). *Dishonesty in the workplace: A manager's guide to preventing employee theft* (pp. 10-11). Park Ridge, IL: London House Press.

4. Carter, D.L., & Katz, A.J. (1996). *Trends and experiences in computer-related crime: Findings from a national study*. Paper presented at the Annual Meeting of the Academy of Criminal Justice Sciences, Las Vegas, NV.
5. Hacker gets time in prison: Former airman downloaded porn. (1999, July 2). *Anchorage Daily News*.
6. Fischer, L.F. (1993). *Characterizing information systems insider offenders*. Proceedings of the 1993 Annual Conference of the International Military Testing Association, Pensacola, FL. Available starting page 289 on <http://www.internationalmta.org/2003/2003Proceedings/03IMTAproceedings.pdf>
7. Web@Work Survey 2002: Cyber addiction in the workplace. (n.d.). Rochester, NY: Harris Interactive, Inc. Survey retrieved March 14, 2004 from <http://websense.com/company/news/research/webatwork2002.pdf> Article is no longer available on the Internet.
8. Towns, D.M. (2003). E-Harassment in the workplace. Article retrieved December 4, 2005, from <http://www.gigalaw.com/articles/2003-all/towns-2003-03-all.html> Article is no longer available on the Internet.
9. Kramer, L.S., Jung, C.G., Gonzalez, J.L., & Richmond, D.A. (2006). *Behaviors and characteristics exhibited by DoD security clearance applicants of counterintelligence concern* (Draft). Monterey, CA: Defense Personnel Security Research Center.
10. Richardson, R. (2003). *CSI/FBI Computer Crime and Security Survey*. San Francisco, CA: Computer Security Institute.
11. Bridwell, L. (2003). *ICSA Labs 8th Annual Computer Virus Prevalence Survey*. Herndon, VA: TruSecure Corporation. Retrieved March 14, 2004 from <http://www3.ca.com/solutions/collateral.asp?CID=41607&ID=4349>
12. Fischer, L.F. (1991). The threat to automated data systems. *Security Awareness Bulletin*, 2(91). Richmond, VA: Department of Defense Security Institute.
13. Government Accounting Office. (1991, March 21). *Justice's weak ADP security compromises sensitive data*. Press release of testimony by Howard G. Rhile, Director, Information Management and Technology Division, before the House of Representatives Committee on Government Operations, Subcommittee on Government Information, Justice, and Agriculture.