

Appendix B: CS Department Information Assurance Security Plan and Policy

B.1 Information Assurance Plan

Section 1. General Information

A. Introduction

This document describes how the UI Computer Science Department addresses its computer security needs. It is the official document of correct security practices and the plan for change within the department. It is a living document and is periodically reviewed and revised to meet Computer Science Department needs. All changes and updates are reviewed by the senior system administrator and approved by the CS faculty.

Faculty, staff, and students may use the departmental computer networks to promote scholarship and learning for all students. Ethical standards apply even when material is left unprotected. Users are responsible for understanding and respecting the security requirements of the systems they use and for their own behavior. The department computer usage policy is posted on the department's web page (<http://www.cs.uidaho.edu>), and all faculty, staff, and students using the department's computer networks are required to sign an agreement specifying they will abide by that policy. (Attachment 1)

B. Computer Science Department Security Policy

Users of Computer Science Department computing resources are accountable for their activities and should use only the computers, computer accounts, and computer files for which they are authorized. University and department computer systems and networks may not be used for any unethical, illegal, or criminal purpose. System administrators may suspend computer and network privileges of an individual for violations of this policy, or of local, state, or federal laws.

C. Risk Assessment

A complete security assessment of department networks is planned for the 1999 spring semester. Two graduate students were sent to a specialized course in intrusion techniques and detection on networked systems presented by a major computer security consulting firm, and will lead the effort. However, since the primary missions of the university, and the Computer Science Department specifically, are education, research, and public service, the department networks and computing resources are openly available to all faculty, staff, and students, and are thus somewhat insecure.

D. Plan to Address Discovered Risks

As part of the security risk assessment planned for the 1999 spring semester, a detailed set of recommended actions and a timetable will be developed by the security analysts for review by the Computer Science Department Chair and senior system administrator.

E. Incident Response Procedures

The primary response strategy to intentional intrusions is "protect and proceed." The goal of this strategy is to immediately protect the network upon notification or realization of a

security incident and restore it to normal status so users can continue using the network. A secondary strategy of "pursue and prosecute" will be started with a complete analysis of the event will occur after the system has been restored. The senior system administrator will make use of computer security researchers in the department, within resource limitations.

Section 2. Computer Science Department Security Policy

This security policy is meant to be brief and usable by Computer Science Department faculty, staff, and students. As such, not all eventualities can be documented here. Anything not specifically or generally covered by this policy will be determined by the Computer Science Department Chair, with advice from system administrators, university personnel, legal counsel, as appropriate. Any changes to this policy will be distributed to all department personnel.

A. General

A.1 This policy will be adhered to by all faculty, staff, and students who operate or use the computer systems and networks of the Department of Computer Science. It supplements, but does not replace, existing laws and regulations. Individual labs or faculty members operating their own computers or networks may add, with the approval of the system administrator or Computer Science Department Chair, individual guidelines which supplement, but do not relax, this policy.

A.2 The use of departmental computing and networking resources is for purposes related to the institution's mission of education, research and public service. Accounts are given to and remain in effect as long as the user maintains an official relationship with the department. However, no userid or system may be used for any unethical, illegal, or criminal purpose.

B. Department Privileges:

B.1 The Department Chair may allocate resources in different ways in order to achieve its overall mission.

B.2 The Department Chair has authorized detailed session logging, up to and including complete keystroke logging, of an entire session when necessary to gather evidence of a suspected violation. The department will fully comply with local, state, or federal authorities to provide any information necessary for the litigation process.

B.3 System administrators are empowered to take reasonable steps necessary to preserve the availability and integrity of department computer systems, and to restore the integrity of the system in the case of malfunction, abuse, virus, and other similar situations.

B.4 System administrators may routinely monitor and log usage and session data and may review this data for evidence of violation of law or policy. They may suspend computer and network privileges of an individual for violations of this policy, or of local, state, or federal laws. Administrators have the authority to control or refuse access to anyone who violates institutional policies or threatens the rights of others.

C. Individual Privileges:

C.1 The constitutional right to freedom of speech applies no matter what medium used. Departmental system administrators will not remove any information from individual accounts unless the information involves illegality, endangers computing resources or the information of other users, is inconsistent with the mission of the institution, or involves obscene, bigoted, or abusive language. Users who wish to appeal such removal of information may do so through a letter addressed to the Computer Science Department Chair.

C.2 Access to electronic mail, computer programs, or computer files which are not publicly viewable (through the world wide web or setting of permissions) requires permission of the owner, court order, or other actions defined by law. Access for security reasons may only be done by authorized personnel and only with the approval of the Department Chair.

C.3 Privacy will to be preserved to the greatest extent possible, but users should not expect total privacy of electronic mail (e-mail). System administrators may see the contents of e-mail due to serious addressing errors or as a result of maintaining the e-mail system.

D. Computer Science Department Responsibilities:

D.1 Access to the network, files, application programs, and other system resources will be implemented via a userid and password. System administrators will ensure new users have read and understood this policy before giving access. The system shall have a mechanism that locks a userid after five consecutive unsuccessful logon attempts.

D.2 When system changes in hardware, software or procedures are planned, the system administrators will notify the user community to ensure all users will be aware of the changes and the expected downtime, and to voice any concerns they might have. System administrators will have defined, written procedures for maintaining data integrity during these times. They will also publish a schedule of preventive maintenance for the computer systems.

D.3 Default passwords shipped with servers, operating systems software, or applications must always be changed when the hardware or application is installed or implemented. Software patches to known system problems should be installed as expeditiously as possible.

D.4 System administrators will delete the access of employees or students who are no longer associated with the department as soon as possible. However, users may retain their accounts in limited cases, and on written approval of the senior system administrator.

D.5 System administrators will perform backups on a weekly basis, at a minimum. A copy of these backups should be maintained off-site, in the event of a catastrophic event. However, the department does not guarantee the availability of backups to restore user files deleted through user error.

D.6 The department will take action to provide reasonable protection against environmental threats as flooding, lightning, extreme temperatures, and loss or fluctuation of electrical power. At a minimum, critical hardware should be connected to an uninterruptable power supply.

D.7 The department will take appropriate and reasonable steps to inhibit attempts to obtain unauthorized copies of computer software, computer data and/or software manuals.

D.8 There will be no dial-in capability on department computing resources, or on private computers connected to department networks. Any deviation from this item must be approved in writing from the Computer Science Department Chair.

D.9 System administrators will use available products to provide the ability to trace violations of security to individuals who may be held responsible.

D.10 The department will not act as a censor of information, but will investigate properly identified allegations and will carry out its responsibility to report criminal offenses to the appropriate authorities.

E. Individual Responsibilities:

E.1 Users of Computer Science Department computing resources are accountable for their activities. They must respect the privacy and personal rights of others, to include abiding by all applicable copyright laws and licenses, and refrain from behavior which impairs the institution's reputation within the community. They should use only the computers, computer accounts, and computer files for which they are authorized, and for the intended purpose.

E.2 Passwords should be chosen by and known only to the individual user responsible for the userid, and not written in an easily discoverable location. They should be non-trivial passwords, consisting of a combination of uppercase and lowercase characters, numbers, and special symbols.

E.3 Users are responsible for assisting in the protection of the systems they use in the Computer Science Department. This includes, but is not limited to:

- E.3.1 Using available mechanisms and procedures to protect their programs, software libraries, and data,
- E.3.2 Properly (re)setting protection levels to their files and directories
- E.3.3 Reporting possible security lapses on department systems to the system administrators
- E.3.4 Not loading software or data from untrustworthy sources (such as freeware) or software that allows access through the network to the contents of files, without permission from the senior system administrator
- E.3.5 Not giving others access to any system they do not administer

E.4 Private workstations, personal computer, or other devices may be attached to the department network with the consent of the senior system administrator. However, the owner of a privately owned machine is responsible for the behavior of the processes running on that machine and all the network traffic to and from the machine. Further, private machines may not be used as a router to other networks or systems, to provide network access to individuals who would not have had access through official departmental systems, or for commercial gain or profit.

E.5 Hard copy output devices are not printing presses. Users may only print academic and school-life related work.

E.6 Users should not display in shared facilities images, sounds or messages which could create an atmosphere of discomfort or harassment to others, and refrain from transmitting to others inappropriate images, sounds or messages which might reasonably be considered harassing.

E.7 Workstations must be logged off or secured to a point that requires a new log-on whenever they are unattended. Users should not prevent others from using shared resources in open use labs by placing signs on devices to "reserve" them without authorization.

E.8 Users are strictly prohibited from the following activities, unless they are being conducted as part of valid coursework or research. In such limited cases, the users must gain permission from the responsible faculty member and the senior system administrator.

- E.8.1 Do not use department computers, network facilities, or resources in the commission of a crime.

- E.8.2 Do not access or modify the files or directories of other users (including those belonging to root or system administrators), or attempt to secure or modify their system privileges.
- E.8.3 Do not attempt to gain illegal access to computers, network facilities, information services, or resources within this department, or use the department's computing systems to gain unauthorized access to computing accounts or systems outside the department's systems.
- E.8.4 Do not intercept, monitor, or decrypt system or user passwords or access control information, or secretly collect information about other users.
- E.8.5 Do not use mail facilities to send rude, obscene, harassing, or illegal materials, or modify information in the mail facilities to misidentify yourself or hide your identity
- E.8.6 Do not run or otherwise configure software or hardware to intentionally allow access by unauthorized users, alter or avoid accounting and audit trails, disguise your identity, or deliberately degrade system performance.

Section 3. Risk Assessment of Computer Science Department Computing Resources

A. Overview:

A complete security assessment of department networks is planned for the 1999 spring semester led by two graduate students specialized knowledge intrusion techniques and detection on networked systems. Since it is the first formal assessment we have done, it is expected they will find a variety of security flaws, especially given the university and department missions of education, research, and public service. Their primary responsibility is to identify the flaws and associated risks so the Computer Science Department Chair and senior system administrator can decide the appropriate actions to either resolve, mitigate, or accept each risk individually. The form expected to be used is Attachment 2.

The remaining parts of this section will identify some key questions to be answered as part of the assessment.

B. Natural Disasters and Perils:

B.1 Are there reasonable preventative measures to protect equipment and data in natural disasters or perils, such as power loss, excessive heat, falling water, etc?

B.2 Are there documented restoration actions for system failures, either catastrophic or minor?

B.3 Are tape backups kept off-site in the event of catastrophic failure?

C. Security Procedures:

C.1 Is the policy on granting access and educating users followed?

C.2 Are lines of responsibility and boundaries clearly identified?

C.3 Are there procedures in place to address newly discovered vulnerabilities?

C.4 Training plan so that everyone knows their responsibilities, with a timetable

C.5 Are critical nodes, data, and assets identified and prioritized for faster restoration?

D. Physical Security:

D.1 Are potential high-value assets reasonably secured from theft?

D.2 Do potential intruders have open access to computer systems or networks?

D.3 Are there appropriate methods to dispose of sensitive media (shredders, degaussers, overwriting, etc.)?

E. Computer and Network Intrusions and Misuse:

E.1 Are there dialup capabilities the system administrators are not aware of?

E.2 Is password shadowing implemented, or is there a periodic check to see if user passwords are easily cracked? (It is estimated 80% of all network security problems are caused by bad passwords.)

E.3 Are policy violations detectable, either by automated or manual means?

E.4 Are all recent vendor patches installed, especially the security-related ones?

E.5 Were the intruders/analysts able to gain access? How?

Section 4. Plan to Address Discovered Risks

This section will not be done until after the risk assessment is completed. This plan will identify recommendations, and appropriate action plans, with accountability, milestones, time required, and judgement of results. The plan will be extensible, allowing for change and growth.

Section 5. Incident Response Procedures

The primary response strategy to intentional intrusions is "protect and proceed." The goal of this strategy is to immediately protect the network upon notification or realization of a security incident and restore it to normal status so users can continue using the network. While potential intruders and computer crackers may realize they have been discovered, and be able to take actions to avoid being traced, the main interest of the department is to restore service to the users.

System administrators will take the following steps in accordance with the policies identified earlier within this plan:

- 1. Actively interfere with the intruder's actions, if they are ongoing.
- 2. Prevent further access by that intruder, if this can be done quickly.
- 3. Immediately restore the network to normal operation, if possible.
- 4. If normal operations are not immediately possible, then isolate network systems and bring critical systems operational first.
- 5. Notify the Computer Science Department Chair and the senior system administrator as soon as possible.
- 6. Document all actions taken, including files modified, phone calls made, or processes stopped.
- 7. Notify users and the appropriate personnel at the University of Idaho Computer Services Department.

A secondary strategy of "pursue and prosecute" will be started with a complete analysis of the event will occur after the system has been restored. The senior system administrator will make use of computer security researchers in the department, within resource limitations.

- 1. Make a mirror image of the drives which may have been affected by the intruder(s). This is required to try and preserve the evidentiary trail for later prosecution.
- 2. Enlist the help of faculty and graduate computer security researchers.
- 3. Analyze log files, audit trails, and all other pertinent information to determine the extent of intruder actions and the entry points the intruder used.
- 4. Keep Computer Services informed of progress during the investigation stage.
- 5. Identify appropriate law enforcement agencies for possible prosecution.

B.2 Computer Usage Policy

Adopted February 10, 1994

1. Introduction

This policy governs use of computers and related equipment operated by the Department of Computer Science of the University of Idaho. Each computer user is a member of a community; the purpose of this policy is to maximize the value of our resources to that community. The intent of the policy is to permit maximum freedom of use consistent with State Law, University policy, and a productive working environment. The policy applies to all those who use CS computers. Depending on the seriousness of an offense, violation of the policy can result in penalties ranging from reprimand to loss of account to referral to University authorities for disciplinary action.

2. State Law and University Policy

Use of CS computers must comply with Idaho law and University policies. Therefore, CS computers may not be used for commercial or profit-making purposes, for political purposes, or for personal benefit where such use incurs a cost to the Department and is not academically related.

State law prohibits unauthorized access to computer systems. Access of or attempts to access another person's directory, files, or mail, whether protected or not, without permission of the owner is prohibited. Attempts to access unauthorized machines via the computer network, to decrypt encrypted materials, or to obtain privileges to which the user is not entitled are prohibited. The University has signed software licenses for much of the software that is available on CS computer systems; removal or transfer of such software without authorization is prohibited.

This policy statement authorizes CS computer systems staff to examine the user's files if required as part of their official duties.

Sharing of a computer account with other persons is prohibited; each user must have an individual account. Passwords must be protected, and the user must not leave a machine logged on when the user is not present unless the machine is in a secure area, such as a private office. [UI Computer Services Policies](#)

3. Working Environment

Users of CS machines should conduct themselves in a manner that promotes a productive working environment. Conduct that creates a disturbance to other users is prohibited; this includes making noise, taking beverages into the computer labs, and printing or displaying materials that are unsuitable for public display. Conduct that intentionally or negligently interferes with the proper operation of the system or its use by others is prohibited.

Users of electronic mail and bulletin boards shall not send messages that are libelous, patently offensive, or that intimidate, threaten, demean, or harass individuals or groups, or that would otherwise bring discredit to the University or the Department.

4. Use of Resources

Users of CS computers shall not consume unreasonable amounts of limited resources. Resources that are in limited supply include laser printing, disk space and, in some cases, machine access itself. Laser printing should be used judiciously; it should not be used for multiple copies. Picture files or other large files should not be stored on disk unless they are academically relevant. Playing of games and other non-academic activities should be restricted to periods of off-peak usage. The Department may impose restrictions or limits on use of resources.

5. Questions

A student, staff member, faculty member, or system administrator who is unsure about how to deal with questions about any aspect of this department computer use policy should contact the chair of the Department of Computer Science at (208) 885-6589 or chair@cs.uidaho.edu.