Chemistry and Biochemistry Department
Computer Management Policy

May use the CTRL+F function to find what you're looking for; use key words or the titles of the appropriate section

Table of Contents

Chemistry and Biochemistry Department
Computer Management Policy

Chemistry and Biochemistry Department
Computer Management Policy

1. Need for Computer Management Policy

There are three key reasons for establishing a computer use and management policy for the Department of Chemistry and Biochemistry. These are listed and explained as follows:

1.1 Cost efficiency in the use of university and research funds is in the best interest of all in the department.

Department records indicate that an average of about $250,000 per year has been spent on computer hardware and software in the years 2000, 2001 and 2002. Any purchases outside of the department purchasing structure would increase this figure. The costs of individual purchases have sometimes been considerably higher than that available through university contracts or through quantity purchases. For example, price reductions of up to 80% have been obtained on some multiple-user or university licenses. In addition, maintenance contracts have also been greatly reduced. There is sometimes a wide range in the cost for software products which all purport to accomplish about the same function. These issues deserve our serious consideration. The CSR office is regularly working with OIT, purchasing, other university units, and directly with companies to secure additional university discounts.

1.2 Improved efficiency in the use of time required for computer support is in the best interest of all in the department.

The productive use of computers for scientific applications, office production, and communication depends on several critical steps including installation, configuration settings, and compatibility with instruments and the software tools being used by others. The establishment of procedures and practices that anticipate and minimize the likelihood of delays and other problems in these critical steps will benefit faculty, staff, and the CSR personnel.

The many diverse computer applications that are in use in the department make the work of the CSR staff challenging and often inefficient. The more we can elect to use common hardware and software the more efficiently the CSRs can work, which will benefit all in the department.

In a number of instances, the hardware warranties, the source media for a software application and the user manuals have been lost. This has lead to disappointment, delay, and added expense when changes are made to the system or the application was lost from the computer for one reason or another. An organized system for filing software source media, warranties, and instructions would greatly facilitate efforts by the CSR to support individual faculty and their computer needs.

In many instances when users have installed hardware/software themselves, it has not interfaced properly with the department network and the CSR office has been called on to make adjustments in the settings. It usually would have been more efficient for both the user and for the CSR to have the CSR office install the hardware/software.

1.3 Compliance with software license agreements needs to be the department policy for both moral and legal reasons. BYU, as well as individuals, are financially liable for all illegally installed software.

It is very easy to be unaware of software license violations and to rationalize the improper use of software. However, the use of software in violation of the license agreement is not in harmony with the moral principles we espouse and is as incorrect as shoplifting.

The BYU policy regarding this issue is as follows. "All members of the BYU community--faculty, staff, students, volunteers, and patrons--are expected to respect the rights of copyright owners as established by relevant state and federal laws. Members of the BYU community who disregard the Copyright Policy may be in violation of the Church Educational System Honor Code; may jeopardize their employment; may place themselves at risk for possible legal action; and may incur personal liability." (Executive Summary, Copyright Policy, University Electronic Handbook)

The discovery of noncompliance with copyrights could lead to stiff fines, loss of favorable license agreements for the department and university, and considerable embarrassment for the department, university, and the church.

The software on our computers comes from the manufacturer or is loaded by the CSRs, the department staff and faculty, or by students. One purpose of a software policy is to establish procedures that will improve our ability to comply with license agreements and to verify compliance when requested to do so.

It is likely that some software programs were purchased and installed according to the license agreement, but that the program media and records of the purchase have been lost. However, under the law programs are assumed illegal unless the media or proof of purchase can be produced.

2. Purchasing Hardware

The CSR Office should be involved in all acquisitions of computer hardware including those purchased using external research funds, gifts to the University, and equipment here on a loan agreement. They need to evaluate the total cost of the acquisition to the Department including support and maintenance expenses.

2.1 Coordinate all purchases through the CSR Office

The CSR Office can take advantage of quantity discounts, purchasing contracts, and special buying opportunities to reduce the cost of computer purchase. They also are aware of the specifications needed to interface the equipment to our network infrastructure. They can provide excellent advice on the reliability of manufacturers and the breakdown record of their products.

Many commonly needed computer hardware parts and supplies are available in the department.

The CSR has available monitors, keyboards, mice, cables, and other commonly requested items. Some items are new and some are used. Not only are these items conveniently available, but they are much less expensive than purchasing them some other place.

The Chemistry Central Stockroom has CDR, CDRW, and floppy disks. In addition, they also carry ink jet printer cartridges for the commonly used printers in the department. They are priced lower than other commonly used sources for these items.

It should also be remembered that the instrument shop people will repair laser jet printers and they have toner cartridges for laser printers. We should get all of our toner cartridges from the instrument shop.

The CSR can help with the decision on purchasing extended warrantees when available. Many times the cost of the warrantee is small compared to the cost of the CSR's resources.

Equipment given or loaned to the Department must meet similar requirements of reliability and supportability as new purchases. Just because a computer is given to the Department doesn't mean that it will be free to operate. The support and maintenance costs can easily cost more than a new computer. The CSR must approve all equipment being given to or loaned to the Department.

3. Purchasing, Developing, and Customizing Software

Faculty and staff should have as much freedom as possible to select the software programs that best serve their needs. The CSR office needs to review all software acquisitions to make certain they will not affect the operation of other programs and that they will be compatible with the operational hardware. The University provides a standard suite of software that is to be used whenever it is possible. The CSR office will not be responsible to maintain or service any software installed contrary to the policy stated below.

3.1 Software Acquisition

Department Infrastructure. The CSR is responsible for acquiring, developing, and/or customizing all software used to support the Department Infrastructure. If the software can be procured from a commercial source, the CSR will make a recommendation to the Department Chair on the best source to satisfy our needs and to receive funding approval. Usually the guidelines discussed in section 3.6 below will apply. If the software needs to be written or existing code modified, then the CSR will present to the Computer Committee an estimate of the time required for the project and its impact on the Department. The Computer Committee will determine the priority of the work compared to those already approved. All campus resources will be considered in determining the most effective method to develop the software including: using student employees under the direction of the CSR, requesting CID or IMC support, and selecting an off-campus programmer to write the software. The Computer Committee will then make their recommendation to the Department Chair for final approval and funding.

Faculty/Staff. Faculty and staff needing to acquire software to support their academic classes or research programs should present their requests to the CSR for review before proceeding with the suggested software acquisition. The principles discussed in section 3.6 below will apply. Acquisition requests that cannot be filled with developed software will be referred to the Computer Committee. The Computer Committee will make their recommendations to the Department Chair on the most effective mechanism to be used and the relative priority compared with other needs in the Department. Priority will be given to those projects with enough approved funding to complete the project. The CSR will be consulted in writing about the software specifications needed to efficiently complete the project. In general, the CSR will not be asked to develop these software projects but will act as an adviser to insure the software will perform successfully on our network. The Department Chair will make the final decision on which software will be developed.

Software installed on any Department computers without receiving the above approvals will not be supported by the CSR office. Computers with unapproved software installed will receive the lowest priority for maintenance by the CSR office.

3.2 Software associated with Network Servers, Switches, Storage Hardware, and Other Network Devices.

All of the software used on the department network will be preinstalled on the computers at the time of purchase or will be installed under the direction/approval of the department's CSR office.

The CSR office will keep a library of all network software that will include the distribution media, instructions for installation, and the software license agreements.

The CSR office will arrange for renewal of network software licenses.

Disciplinary action may by taken by the Department Chair against any person attempting to modify existing network configurations or installing unapproved software that interferes with the function of the network.

3.3 Software associated with Student Computer Laboratories

Computers in the following student laboratories are included into this category: the W-152 lab; the C-231 lab; and C-131, C-131A, C-149A, C-188, and C-194.

All of the software used on these computers will be present on the computers at the time of purchase or will be installed by the department CSR office.

Prior to each semester or term the department faculty will request the software needed by submitting the request form accessible from the department web page. (See W152 Lab Software Request)

The CSR office will keep a library of all software that will include the distribution media, instructions for installation, and the software license agreements.

The CSR office will arrange for renewal of software licenses.

Unauthorized software will be removed from these computers.

3.4 Software associated with Faculty, Staff and Research Computers

This includes all other computer equipment purchased with BYU or grant funds.

The purchase and acquisition of all software will be coordinated through the CSR office. A phone call or e-mail early in the decision process will prove to be an efficient benefit. Green requisitions must be submitted for all computer-related purchases. The CSR office is simply performing the same function for software and hardware that the department purchasing agent performs for chemicals and equipment. The CSR staff has the responsibility of informing faculty and staff of the status of all orders for computer related items placed through the CSR office. Purchase orders will automatically be reviewed by the CSR. In addition, please coordinate prior to all Internet and private purchases.

As a rule, CSR personnel will load new and upgraded software. However, the CSR personnel should be consulted in cases where it is reasonable for someone else to load the software. This will make efficient use of department human resources and ensure compatibility with the department network. *The CSR office must be informed of all software being installed on our department machines.*

The CSR office must have on file a complete copy of purchase information, the license agreements, and the original media when it is part of the purchase. The CSR Office also encourages users to provide a file copy of the documentation and instructions for all software being used in the department. Faculty and staff may retain an archival copy of the media. This procedure will demonstrate departmental compliance with license agreements. It will also prevent the expense and inconvenience of lost software and documentation.

The use of computers for personal purposes is acceptable as is the use of an office or desk. This use is considered as nominal use as long as it does not interfere with an individual’s ability to fulfill the expectations of the university position. The personal use of the computer must comply with university regulations. If software for personal use is to be loaded on the computer, two conditions must be satisfied. First, a complete copy of purchase information and license agreement must be on file in the CSR Office. Second, the software must not interfere with the network or cause a network security risk.

File sharing or peer-to-peer software **must not** be installed on any machine within the department network. Examples of such programs are: Kazaa, Bearshare, Morpheus, etc. Some of the reasons for this restriction are as follows. 1) These programs are designed to violate copyright restrictions. 2) Such programs often make use of the memory, disk space, computer time, and the network for operations over which the user has no control. 3) These programs often contain spyware, which tracks all of the Internet sites an individual computer visits. 4) Such programs will overload both the department and university networks.

3.5 Software associated with Computers Owned by Individuals, used in the Benson or Nicholes Buildings and connected to the Department Network

A computer owned by an individual may be connected to the department network if it is properly registered. Every personal computer must have active virus protection software installed. Virus protection software provided under the university license is available without charge to all full-time employees. All software used on a personal computer must not pose an unusual hazard to the department network. All peer-to-peer software must be removed or disabled.

If software on the personal computer is outdated, unusual, or unfamiliar to the CSR office, it becomes the responsibility of the computer owner to provide the computer hardware and software that is compatible with the department network.

If the computer is to be used for research, teaching, or similar professional work, the CSR office may make a limited effort to fix the software so that it will work efficiently with the department network. This assistance is provided on a time-available basis and takes second priority to their normal duties.

All software for professional applications must comply fully with university and department policies and copyright agreements. Documentation of proper ownership must be provided upon request.

If a personal computer cannot meet these conditions, the owner will be requested to remove it from the network.

3.6 Software Standard Recommended by the Department.

There are several hundred software packages being used in the department at the present time. The CSR personnel cannot provide efficient and knowledgeable support for all of this software. Therefore, out of necessity, the following systematic approach to software acquisition, installation, and support has been developed. It involves a three-tier classification of software. It also involves a dynamic interplay involving the responsibility of CSR personnel, their support for software applications, and the responsibility of faculty and staff for determining how to use their software. The CSR staff has full and sole responsibility for network hardware and software. Faculty and staff are fully responsible for the application of their specialized software. In between these two is the dynamic arena of shared responsibilities. The three-tier classification will help to organize the shared responsibilities.

A considerable efficiency in purchase cost, installation, maintenance, data sharing, and instruction is expected when a standard set of software is used as much as possible. For this reason, the department will identify a software standard that is strongly recommended. The major uses of software in the department are for routine functions required by nearly everyone. There are also software functions or applications that are common to specific groups of people within the department. Therefore, it is possible to recommend a software standard for a number of functions.

Tier 1 software. This is the standard software recommended for use in the department. Much of this will be provided automatically when a new computer is installed. This software will be purchased with the computer hardware or provided by the university or department. The CSR office will see that the software programs are available, and they will have made arrangements for the licenses. The maximum CSR support will be available. However, the CSR office cannot train users in all of the applications, nor is it their responsibility to customize the software (such as writing Macros) to meet individual needs. However, the CSR will be happy to advise faculty, staff, and students on alternative assistance options they can use for their programming needs.

Tier 2 software. This includes software presently preferred by some workers or programs used by a considerable number of people. It could include software that has many functions in common with the Tier 1 software, but some features for which the user is willing to pay a premium. The CSR office will usually have this software available at a cost that has been negotiated to be as favorable as possible. The CSR personnel will provide good support but will not be prepared to support this as completely as for Tier 1 software. For example, problems with file sharing that arise because of using Tier 2 software will be the primary responsibility of the user.

Tier 3 software. This will include all software that is not classified into Tiers 1 and 2. The CSR office will assist in acquiring and installing this software and in giving a nominal amount of support. However, solving problems that arise in the installation and use of the software will be the primary responsibility of the user.

Appendix 1 lists examples of software classified into the three tiers but this list is expected to be dynamic with changes taking place frequently.

3.7 Compliance with Software License Agreements

It is the department and university policy to use each software package in compliance with the license agreement under which it was distributed. Every computer in the department falls under the supervision of a faculty or staff member. Therefore, the primary responsibility for using software according to license stipulations rests upon the full-time faculty or staff member responsible for the computer. Each staff and faculty member is obligated to carefully read the agreement, to know the allowed use, and to abide by that agreement. Each person *using* or *installing* software also has a responsibility to understand the license.

The following information about every software purchase is to be on file in the CSR office: 1) Proof of purchase, 2) license agreement, 3) copy of the software distribution media, and 4) copy of the software documentation. The CSR office will have the necessary information for software covered by purchasing and license agreements the university has negotiated with various software suppliers. Faculty and staff are responsible to provide the CSR with the materials for other software packages.

The CSR office staff carries a heavy responsibility for compliance with software license agreements. They install and service a significant number of software applications each week. They are also in a vulnerable position if our department were audited for compliance with software license agreements. They cannot install or service software for which there is no proper documentation or which they believe is being used contrary to license agreement. The default assumption is that a properly purchased software package is to be installed on only one computer unless the written license agreement clearly indicates differently.

CSR personnel will use their experience, training, and judgment in advising and assisting department computer users. They are not in a position to police and enforce this license policy. The department should be able to rely on self-policing. However, when the CSR office becomes aware of software that they feel is being used in violation of the license, they will bring this to the attention of the faculty or staff member. The situation should be corrected within a few weeks. In some cases there may be room for differing opinions on an interpretation of the license and on the honest application of the agreement. Such cases may be brought to the computer committee or to the Department Chair for a final judgment.

4. Use of University Owned Computer Equipment

The Department of Chemistry and Biochemistry will make every reasonable effort to maintain the Department and University computer network as a wholesome tool for academic, scholarship, and university business purposes. Students, faculty, and staff have a right to expect that computer workstations within the network system will be free of objectionable material.

It is contrary to the BYU Honor Code and department policy for faculty, staff, or students to knowingly access computer web sites that contain pornographic and other material including visual images and text that are inconsistent with the BYU Honor Code. These websites might include those of groups promoting gambling, racial hatred, sexual discrimination, bomb building, violation of federal, state, and local laws, and values inconsistent with the church teachings. It is also improper and contrary to the honor code to participate in computer chat rooms where lewd and sexually titillating or explicit language is used in the conversation. Further, it is illegal to carry on such correspondence with a minor. It is also illegal to be involved in child pornography. Violators of these laws may be convicted of criminal charges. It is recognized that objectionable web sites may inadvertently be accessed from time to time. It is the obligation of the computer user to immediately close the site or, if necessary, turn off the computer.

The Department of Chemistry and Biochemistry will implement the following procedures to achieve the computer environment discussed above.

4.1 General Department Procedures

Chemistry and Biochemistry Department
Computer Management Policy

The following message will appear as a prominent feature on the computer as part of each login procedure. This message must be cleared before the login procedure can progress.

Usage of this computer is bound by adherence to the BYU Honor code.

ALL INTERNET ACCESS IS MONITORED by room number and username.

Any violation of the HONOR CODE, especially the accessing and/or viewing

of pornographic material or improper involvement in chat rooms, will result in a loss of computer privileges and immediate referral to the Honor Code Office. Repeat offenders will be dismissed from all programs and employment in the Department of Chemistry and Biochemistry for a year. Anyone found accessing child pornography will be referred to the campus police for possible criminal prosecution.

All faculty members are encouraged to place in their course syllabus a warning similar to that in the paragraph above and to mention the policy during their first class. A warning will also be placed in the Graduate Student Handbook.

Procedures for the use of computer login names and passwords on all department computers will be followed as specified in section 6 of this document. Users who login are responsible to logout when they leave the vicinity of the computer for more than 30 minutes. Some computers in research laboratories where access is limited may remain logged in unless violations of this policy occur.

The department Computer Service Representative (CSR) will maintain equipment and software that will alert the CSR when there is a sustained and/or repeated access to computer sites or chat rooms displaying pornography or other material contrary to the Honor Code of the University.

When there are indications of access to an improper web site, the CSR will determine the room, MAC address of the machine, and login name. He will report the incident to the department chair or an associate chair as soon as possible. The CSR will also provide the evidence required by the department and by the Honor Code Office. If it is not possible to determine the person involved, the CSR should notify the department chair and the faculty member responsible for the area in which the incident took place.

4.2 Working with Individuals Who Access Inappropriate Web Sites

Faculty and Staff members, including post doctoral fellows, will be reviewed in light of university disciplinary procedures and the qualifications required for continued employment at BYU.

All cases of inappropriate internet access will be reported to the Department Chair or an Associate Chair. After consulting with the responsible faculty or staff member, an Associate Chair will interview each student suspected of accessing inappropriate web sites. One Associate Chair will handle all of the undergraduates referred by the CSR and the other Associate Chair will handle all of the graduate students and postdocs. It is important that only one person handle all such cases so that the treatment of students is consistent and in accordance with university and department policy. The Associate Chair will refer the student to the Honor Code Office and provide the student with a letter specifying the violation, the requirement to receive counseling, and to require a written confirmation that counseling is taking place. The letter is to be signed by the student. Any students or faculty members found accessing child pornography will be referred to the campus police for possible criminal prosecution. In every case involving a graduate student or an undergraduate student in research or otherwise employed by the department, the supervising faculty member will be notified of the problem by the Associate Chair.

Students will always be referred to the Honor Code Office and their discipline will then be determined in the light of all information available from the department and the Honor Code Office.

First-time offenders in the department **may** be allowed to continue their academic program and employment in the department and university. Second-time offenders **will be dismissed** from all access to department academic programs, equipment, and employment for a year. Their registration for chemistry and biochemistry courses will be blocked for a year. In some situations, dismissal for more than a year may be warranted.

Offenders will be required to have counseling with their bishop and/or a professional counselor as determined by the Honor Code Office. The Honor Code office will provide, upon request from the department, an indication of the offender’s compliance with the counseling specified by the Honor Code Office. A first-time offender who is not complying with the counseling specified will be blocked from department programs as indicated in the paragraph above.

4.3 Personal Use

Although the -University allows for personal and ecclesiastical use of computer resources, including their use in network communications, it expects such use to be minimal and should not occur under circumstances that interfere with University or personnel work responsibilities or that inappropriately consume finite resources. Mass mailings using the email system for personal communications should be approved by the Department Chair in advance.

4.4 Advertising, Selling, and Soliciting

Use of computer and electronic communication resources for advertising, selling, and soliciting is prohibited without the prior written consent of the Department Chair. Any such uses must comply with the University=s Advertising/Selling/Soliciting Policy.

5. Repair/Support/Maintenance

Requests for computer support can be made by calling the CSR office (422-5771), sending an email request (csr@chem.byu.edu), or submitting a service request on their website (http://chemwww.byu.edu/computersupportservicerequest.php). Please do not call them at home or go to their home asking for assistance. Any calls to their homes should come from the Department Chair or Associate Chair when there is an emergency on the network. Please respect their family time and privacy.

Computers owned by BYU but checked-out to faculty and staff to operate at a remote location must be returned to the Benson building to be repaired. These machines are lent as a courtesy to the employee and do not carry a promise of off-site maintenance. Many of them are older models and require above average maintenance times. The CSR office cannot take the time to travel to homes to repair these machines.

6. Department Password Policy

Chemistry and Biochemistry Department
Computer Management Policy

All computers connected to the network must have adequate password protection. Passwords are the first line of defense in order to maintain the security of the department network from unwarranted intrusion and unauthorized uses from outside entities. Therefore, it is necessary that a policy be implemented that safeguards the passwords used by authorized users of the department network. Given below are guidelines that all users of the department network are expected to follow:

- Passwords will be composed of at least 6 characters and no more than 20.
- Passwords will contain a combination of both alphabetic **and** alphanumeric characters.
- No part of the password will contain a word (or a derivative thereof) found in the dictionary nor will the password contain personal names.
- No part of the password will contain sequences or patterns of letters or numbers.
- Passwords will be changed 3 times a year.
    - At the beginning of winter semester.
    - At the beginning of spring term.
    - At the beginning of fall semester.
- All passwords sent over the network both internally or externally will be encrypted. There will be no open transmission of passwords.

7. Antivirus requirements

Most of the infections on our network have come from screen savers, greeting cards, pictures, interesting stories, and other non-business related information. If you receive these unsolicited, immediately delete them. If you are on mailing lists where you get these types of mass mailings, then have your name removed.

Have your virus software automatically updated at least once per week. The university has already paid for the Norton Antivirus Software program for every computer in the department. If you have any questions about installing it on your machine, contact the CSR office

Do not use software or data disks in your machines unless one of the following conditions has been satisfied:

a. It has been checked thoroughly for viruses,
b. It comes on an original distribution disk from a reputable manufacturer, or
c. It is software you have authored using a computer protected by an antivirus program and can vouch for its safety.

The CSR office can help you if you have any doubts.

If you receive an email that looks questionable, then contact the sender before you open it.

The recommended mail program for our department is Eudora. The majority of viruses will not propagate using the Eudora software. If you choose to use another mail program such as Outlook Express and your machine is responsible for infecting others in the department, then the CSR office will require you to change to Eudora.

The department network and computers are provided for business use. Nominal personal use of these resources is acceptable. However, personal use should not include activities such as sending large graphic or music files that slow down our network.

Computer viruses are becoming more sophisticated and more destructive. Our computer network is one of the most important tools we use in the office. Using a good antivirus program and following the above guidelines well help keep our network free of disabling viruses.

8. Backup policy Overview

Data files generated both in teaching and research are crucial to the functions of the department. As a department we need to make sure that all data is properly backed up in order to make sure that this data is not lost. The primary responsibility for this belongs with the user. Each person in the department can make sure that data is saved in multiple locations (such as on a local disk and on the department file server) so that the chances of loss are minimized. The department will also provide facilities to write data to a permanent media, such as a CD-ROM or DVD-ROM disk, so that individual users can make permanent copies of their files. The CSR office maintains department file servers for faculty, research and student needs. File space on this server will be made available for storage, and files stored will be backed up on a regular basis. Finally, a mechanism will be created for archiving important data.

8.1 Definitions

When developing policy for computer file backup, we will define two different types of backup.

1. Disaster Recovery

Disaster recovery is important when data is lost as a result of a hardware failure. The goal of this is to restore the lost data up to the point in time of the hardware failure.

2. Archiving

Archiving is important either when the data cannot be stored as normal files (for example because the files are too big) or when files have been accidentally deleted and need to be recovered. The goal here is to guarantee that important data is always available.

8.2 Desktop and Laptop computers

Given the rapid growth in the size of computer hard drives, backup media, such as tapes, have not kept pace with capacity. This makes it difficult to provide a simple backup procedure. In most cases the majority of data on a hard drive is programs and program data, which can easily be reinstalled in the case of a disaster, and which does not need to be archived. Computer users will be responsible for identifying what data on their computer need backing up, since they know best what files are irreplaceable. Users should keep copies of this data either in a permanent media, such as a CD-ROM or DVD-ROM, or on the department file server, or both. This data will then be quickly accessible in cases of local data loss. The CSR office will keep original media of software available so that a computer can be quickly rebuilt with necessary programs, and the data files copied back from the server or other media. In implementing this policy, the department will provide:

1) File space on a department file server for users to archive data

2) A means for creating archival media copies of important data at the request of users

8.3 Department File Server

Given the importance of computer data, the department will provide a secure and fully backed up file server. This server will have sufficient performance and capacity to meet the needs of the department. This system will store all files in a redundant fashion, such as a RAID 5 array to make sure that data is not lost in the event of a disk failure. Backup of the server needs to be considered both from a disaster recovery and an archiving standpoint. The total amount of data stored on the server is large in comparison to any available archival system (in its current incarnation it would require 500 DVD-ROM disks to provide a backup for the entire array), so it is necessary to consider the importance of specific data. On the server it will be the responsibility for users to mark data directories as being necessary to archive or not. Data which is marked as needing to be archived will be copied to an external hard drive. The CSR office will store a disk containing important information in an off-site location in the case of a major disaster. In implementing this policy, the CSR office will:

1) Make a disk backup of data on the server marked for archive at least every 48 hours

2) Keep multiple copies of backup data, maintaining data for at least one week.

3) Maintain an off-site storage of data which is at most one month old.

9. Risk Identification

The Department of Chemistry and Biochemistry Computer Committee will meet on a regular basis (at least monthly) to discuss and review potential risks to the department network. As risks are identified, the 5-year plan will be updated to incorporate changes needed to address those risks in a timely manner.

10. Private Computer Support

We have over 700 computers in our Department that the CSR office is being asked to maintain in addition to their normal responsibilities to operate, maintain, and upgrade the network. Our CSR office does not have the time or resources to repair/maintain private computers even though they may be used for BYU business or are required for a class assignment. Students, faculty, and staff may bring in their own computers and plug them into the Department’s network providing they do not interfere with the normal operation of the network. However, it is the responsibility of the owner to maintain and repair any problems that may occur when the computer fails to operate as desired. Our computer support staff tries to be as helpful as they can and usually will take time to answer questions about computer problems, but it is only given on a time-available basis. Any exceptions to this policy must be approved by the Department Chair in advance.

11. Requirements for connecting to the network

All privately owned computers that are connected to the Department network must be registered with the CSR office and have current antivirus software installed. Our servers have monitoring software installed that look for virus attacks. If a private computer is detected trying to infect other machines on the network, then the port used by that computer will be disconnected and the registration of the computer will be cancelled. The computer's registration will not be reactivated until the antivirus software has been updated and the viruses removed. Even though all of our computers have antivirus software installed, the network's performance can be drastically curtailed when a few infected machines are trying to spread their virus by sending out a stream of requests searching for vulnerable machines. Most of these problems occur when students have allowed their antivirus software license to lapse.

12. Surplusing old computers

Old computers, not needed to support your work, should be returned to the CSR Office for disposal. They will evaluate the condition of the machine and determine if it can be used in any other applications in the Department. If it is not needed in the Department then it will be surplussed to the University by the CSR Office.

13. Conclusion

The above policies are meant to help us effectively use our computer support personnel and digital resources for the best benefit of the entire department. Our computer support staff has provided outstanding support for our computer resources. They want to continue this same level of service even though our requirements are increasing. By following the above policies we can help them to achieve this goal. If you feel that you have an unusual circumstance that requires support contrary to the above policies, please get approval from the Department Chair before you contact the CSR staff.

Appendix 1
Software Tiers

	PC	**Macintosh**	**Linux / Unix**
Tier 1 This is the standard software suggested for use in the department. Much of this will be provided automatically when ever a new computer is installed. The CSR office will see that the software programs are available with the least expense possible. They will have made arrangements for the licenses. The maximum CSR support will be available. Even here, however, the CSR office can not train users in all of the applications.			
Operating System	Microsoft Windows 2000 Professional Microsoft Windows XP Enterprise	Macintosh OS X (Preferred OS)	Red Hat 9
Office Productivity Tools			
Word Processing	Microsoft Word OpenOffice Document	Microsoft Word OpenOffice Document	OpenOffice Document Abiword
Spreadsheet	Microsoft Excel OpenOffice Spreadsheet	Microsoft Excel OpenOffice Spreadsheet	Gnumeric OpenOffice Spreadsheet
Presentation Software	Microsoft PowerPoint OpenOffice Presentation	Microsoft PowerPoint OpenOffice Presentation	OpenOffice Presentation
Illustrating/Drawing Software	OpenOffice Drawing	OpenOffice	OpenOffice

		Drawing OmniGraffle	Drawing
Personal Database	Microsoft Access	MySQL	MySQL Postgress
Web Browser	Internet Explorer Mozilla	Internet Explorer Safari Camino Mozilla	Mozilla Galeon
Email Client	Eudora Mozilla	OS X Mail Eudora Mozilla	Evolution Mozilla
Anti-Virus Software	Norton Anti-Virus	Norton Anti-Virus	
Utilities	Adobe Acrobat reader QuickTime Microsoft Media Player Dell Open Manage Flash Plugin WinZip ($) Roxio EZ-CD Creator AdAware Direct X SpyBot PanicWare Pop-Up stopper Java Microsoft .net Perl	Adobe Acrobat reader QuickTime Flash Plugin Aladdin StuffIt ($) Toast Perl	Adobe Acrobat reader Flash Plugin Perl

Plotting / Graphing	Origin ($)		
Journal Search Tool	SciFinder	SciFinder	
Chemical Drawing	ChemSketch		
VPN Access	Cisco VPN Client	Cisco VPN Client	Cisco VPN Client
Secure Client	Secure Shell (SSH)	Secure Shell (SSH)	Secure Shell (SSH)
Remote Administration	TightVNC	TightVNC	TightVNC
Tier 2			

This includes software presently preferred by some workers or programs used by a considerable number of people. It could include software that has many functions in common with the Tier 1 software, but some features for which the user is willing to pay a premium. The CSR office will usually have this software available at a cost that has been negotiated to be as favorable as possible. The CSR personnel will provide good support, but will not be prepared to support this as completely as for Tier 1 software. For example, problems with file sharing that arise because of using Tier 2 software will be the primary responsibility of the user.			
Operating System	Microsoft Windows 9X Professional Microsoft Windows NT	Macintosh OS 9.X	Red Hat 8
Office Productivity Tools			
Word Processing	WordPerfect ($) Endnote ($)	Endnote ($)	
Spreadsheet	Quattro Pro ($)		
Presentation Software	Corel Presentations ($)	Keynote ($)	
Illustrating/Drawing Software	Adobe Illustrator ($) Adobe Photoshop ($)	Adobe Illustrator ($) Adobe	

		Photoshop ($)	
Web Browser	Netscape	Netscape	
Anti-Virus Software	McAfee ($)	McAfee ($)	
Utilities	Volo View Secure Shell (SSH) Prizm Plugin ($)	Prizm Plugin ($)	
Development environment	Microsoft Visual Studio Visual Basic Visual C++ Visual FoxPro Visual InterDev Visual Source Safe Active X Data Access ADO, RDS, OLE DB Providers Microsoft ODBC Drivers Jet IISAM Drivers Remote Data Objects and Controls Data Environment Professional Tools Repository Visual Component Manager Graphics Tools API Text Viewer MFC Trace Utility Spy++ Win32 SDK Tools OLE / Com Object Viewer Self-Installing EXE		

	Redistributable ActiveX Control Test Container VC Error Lookup		
Instrument control	National Instruments Lab View		
Chemical Database	Beilstein	Beilstein	
	Microsoft Visio ($) Microsoft Project ($)		
	Palm Desktop		
Plotting / Graphing	SigmaPlot ($)		
PDF Creation	Adobe Acrobat ($)	Adobe Acrobat ($)	
	Organic Reaction Animations		
Virtual Chemistry Laboratory	Virtual ChemLab Organic Virtual ChemLab General Chemistry Lab	Virtual ChemLab Organic Virtual ChemLab	

		General Chemistry Lab	
Tier 3 This will include all software that is not classified into Tiers 1 and 2. The CSR office will assist in acquiring and installing this software and in giving a nominal amount of support. However, solving problems which arise in the installation and use of the software will be the primary responsibility of the user.			
Operating System	Microsoft Windows 3.X OS/2	Any version before 9.0	Any Version before 8.0
Office Productivity Tools			
Word Processing		Claris Works ($)	
Spreadsheet		Claris Works ($)	
Illustrating/Drawing Software		Claris Works ($)	
Plotting / Graphing	Kaleidograph PsiPlot		
Utilities	Adobe FrameMaker ($) Adobe InDesign ($) Adobe Premier ($) Borland C++ ($) Borland Delphi ($) Borland JBuilder ($)	Adobe FrameMaker ($) Adobe Premier ($)	

	Macromedia DreamWeaver ($)		
	Macromedia Fireworks ($)		
	FileMaker Pro ($)	FileMaker Pro ($)	
	Borland Paradox ($)		
	Microsoft Crystal Reports ($)		
	Symantec Act! ($)		
	Microsoft SQL Server ($)		
	Next Page Folio ($)		
	Oracle ($)		
	Waterloo Maple ($)		
	ChemTutor		
	Chem Windows ($)		
	ISIS Draw		
	Mathcad ($)		
	PC Spartan ($)		
	Rasmol		
	ChemDraw ($)		
	MATLAB ($)		
	MiniTab ($)		
	SPlus		
	Crystal Maker ($)		

Home Equipment Policy

Based on the current situation of most faculty having a lap top of some kind for their primary access device and the program the university has for renting computers to students, the University has requested that the practice of providing equipment for a "home office" be discontinued. This item was discussed right after the first of this year in college council and reviewed again in todays meeting. As a clarification please use the following as guideline for current and any future requests for home use.

1. Where possible if there is equipment at home that cannot be currently justified that the majority of use is for work, please have it returned and get any usable computers into the student pool by way of the surplus procedures.

2. At this point in time no other equipment is to be taken home without the proper "Authorization for University Equipment taken from Campus" form signed off by the Chair and Dean's office. The Dean's office will have to be sure there is a real work related need based on clear justification that cannot be met with their laptop and/or a thumb drive. (The CSR's will need to help with this to make sure equipment doesn't just migrate home when replaced. After discussion with the Chair, it can be determined if it's needed in the department first before going through the surplus process to the student rental pool.) It's also important that no equipment leave campus until the proper form is signed off.

Computer Replacement Policy

*Background

*Most computers used by faculty, staff, and administrative employees, are purchased from a special account for access devices. An access device is a computer used to access the network and perform normal day-to-day computing tasks. The University has provided enough money in this account to purchase a new desktop computer every three years for all of our faculty, staff, and administrative employees. They have also funded 80 computers for our student laboratories such as those in C130, C221, C231, C194, and in the Nicholes Building. If an employee needs to purchase a computer that costs more than a standard desktop computer, such as a laptop or high-end desktop computer, then the extra funds must come from other department funds or other employees must purchase computers less frequently. Additionally we have computers in our research and academic labs not funded by the Access Fund that also must be purchased using other funding. We need these computers to support the heavy demand required by our courses and research efforts. In the past, these extra computers have been partially funded because faculty and staff have chosen not to replace their computers every three years or they purchased a less expensive machine than what was allotted.

*Computer Replacement Policy

*The Department will not automatically replace faculty, staff, or administrative employee's computers every three years. Computers will be replaced only when a faculty or staff member submits a budget request asking for a new machine and his or her computer is three years old or older. These budget requests are usually solicited during the Fall semester for the next calendar year. If a department member elects to delay the replacement of their computer, then the funds saved will be either used to purchase additional student laboratory computers or allow others to purchase higher end computers.

Maintenance for computers less than three years old is covered under the initial warranty. Maintenance for computers over three years will be covered by the department's supply budget and be performed on a priority basis.

*Conclusion

*This clarification of existing policy is to allow faculty and staff to make informed choices on computer replacement. The rotation time is left to the individual employee and should be based upon careful evaluation of their computing requirements.

CSR Office Operations

With increasing budget pressures and competition for resources within the department, the chairs' office has asked the computer committee to evaluate the operation of the CSR office and look for ways to increase efficiency. While we know that the proposed changes may be an inconvenience to some, we believe that it will allow the CSR office to provide better support for the department as a whole. Below is a collection of issues that consume an inordinate amount of the CSR office's time. We ask that faculty ensure that they and their research groups follow these recommendations, many of which are already included in existing department policy.

1. /After Hours Service./ Department policy clearly states that faculty and staff will not call or visit CSR support staff (Robert, Michael, or students) at their homes after normal working hours for any support issue. If an issue is truly an emergency, then one of the chairs must be contacted and they, in turn, will contact Robert when circumstances warrant. Faculty, staff and students can send questions or concerns by e-mail to csr@chem.byu.edu <mailto:csr@chem.byu.edu> at any time, and the CSR office will deal with them as soon as possible.

2. /Personal Laptop Computers. /Existing department policy allows personal laptops (including student laptops) to be attached to the department network and be used for research related tasks. However, it should be understood that the service and maintenance of these computers (both hardware and software) are primarily the responsibility of the computer's owner. In order for computers to be used for department tasks, they need to have legal, up-to-date versions of all software, the operating system must be in English, and they must have the university-supplied anti-virus software installed and working. In extreme cases, the CSR office may provide computer support for non-department computers, but they are at the bottom of the priority list and the CSR office may refuse service due to other pressing needs. In particular, many hours are being spent configuring laptop computers to work with the department's wireless network. Clear written and verbal instructions are given by the CSR office as to how this is to be done. In order to use the wireless network, computer owners will need to familiarize themselves with these instructions and make sure that they are not changing necessary settings when they connect to other wireless networks.

3. /Remote Access to the Department Network. /The department network infrastructure currently has the ability to allow remote access to the network drives and other network services. The standard method for remote access will be the VPN network concentrator. The necessary software and written instructions for VPN access can be obtained through the CSR office. Questions about access to specific computers (including the campus supercomputer center, XWindows software, and any other lab specific hardware or software package) or specific applications need to be answered by the faculty or staff member in charge of that resource.

4. /Computer Upgrades. /When upgrading to a new computer or rebuilding an existing computer, it is of course necessary to identify all software and files that must be transferred to the new machine. Since only the computer user can identify which files are important, it must be their responsibility to identify which files need to be transferred. When possible the CSR office will try to make a backup of files but the faculty member should not rely on this backup.

5. /New Computer Purchases. /It is strongly recommended that the standard PC (Dell) or

Macintosh computers be purchased. Non-standard new or used computers may be cheaper at time of purchase, but they constitute a large investment of time by the CSR office to install and keep them running. Where possible the department will try to identify computers in the University surplus system and make them available to faculty members upon request.

6. /Service Priorities./ The service demand on the CSR office is currently beyond its ability to meet on an as needed basis. Department policy has given the CSR office clear and unambiguous service priority guidelines to which they are required to adhere. It is inappropriate to demand or pressure CSR office employees into providing service outside these guidelines. The CSR office is expected to give a good faith estimate of when your service needs will be met. If that timeline and/or priority level is not acceptable, then the department chair should be contacted for a possible exception.

If you have any questions, please feel free to contact a member of the computer committee.

Job Requests for the CSR Office

In order to improve the feedback to faculty and staff on computer related purchases and services, the computer committee has implemented several changes to how jobs should be submitted to the CSR office. The following steps outline how faculty and staff should submit jobs to the CSR office and how the CSR office, in return, will inform the faculty and staff of the status of their requests.

1. All requests for CSR repair services or purchases of computer related items must be submitted by email to CSR@chem.byu.edu or by a personal visit to the CSR office. Faculty and staff should not expect to be able to stop any of the CSR staff in the hall and make a job request and have that be acted upon.

2. For personal visits to the CSR office, Robert or Michael will fill out either a "Green Rec" (for purchases) or a Work Order (for services) and place these in their job queue. Email requests will serve the same function. Requests will be acted upon following established priorities previously adopted by the department.

3. Within 24 hours, the CSR office will send an email back to the faculty (even if a student made the request) stating a summary of the requested action and a best estimate of when the job should be completed. If faculty or staff do not receive this email, then they should contact the CSR office.

4. The CSR office will do their best to inform the faculty and staff of any changes in the completion date for requests, but it is the faculty's and staff's responsibility to track the status of their requests.

We believe following these guidelines will help the faculty and staff be more efficient and predicable in the utilization of the department computer resources.

OEM Software Policy

The policy governing this is the Computer and Electronic Communications policy in the University Policies/Procedures. It in many parts says that we must comply with local, state, federal and international laws and agreements associated with software. Most OEM licenses, are intended for use with the system it is purchased with, and usually come pre-installed. Maintenance of these licenses would be and extreme headache. The specific OEM license would need to be reviewed to see if it is transferable, and removed from the machine it came pre-installed on. If it is transferable, a copy of the license would have to remain with the new computer for license compliance purposes in an audit. Are you ready to create a file of license codes and agreements for every computer you support?

I would strongly recommend NOT using this type of software licensing on University Computers. Software purchased and maintained in the Software Office (Kent Gilberts) has had legal reviews of the agreements and Kents Office has copies of these agreements for compliance purposes. This is also why you report license usage on the IT.BYU.EDU website.

OEM Definition: Original Equipment Manufacturer. A producer that provides a product to its customers, who proceed to modify or bundle it before distributing it to their customers

Printing Policy

We would like to remind everyone about the policy for using department printing resources. I am sure that we all appreciate the support we have for printing and copying, especially in comparison to what most other departments at the university provide and indeed what many chemistry departments at other universities provide. However, we need to make sure that we use these resources judiciously. Whatever we spend on printing and copying must come out of our overall supplies budget—we get no special allotment for printing and copying. On the other hand, we should not feel that we need to restrict our use of these resources in a manner that would hamper effective use of our time.

Please make sure that your students understand that printing allotments are for professional purposes only. They should reimburse the department for any personal printing, just as they should for personal copying. I always point out to my students that faculty also pay for personal printing and copying. Printing is 6 cents/page for B&W; because most students do not have access to a department color printer, we have not set a price yet for color printing, but the library charges 35 cents/page.

Research students using a research computer account are given a 250-page limit each semester. If you think that any of your students needs a larger limit to meet the demands of work for you in a particular semester, you will need to let Robert know (a simple e-mail is sufficient). Printing of drafts of dissertations and theses falls under the professional work category; during the time a student is writing a dissertation, he or she is likely to need a larger limit. Robert has been instructed not to change limits based on a student's word; only faculty or full-time staff may authorize a change. Also, because student accounts are automatically reset each semester, any change in limit will need to be authorized each semester.

Finally, please suggest to your students that they not have as their default choice printing every article they want to read or save. Instead, articles can be saved as pdf versions and only printed out if a hard copy is needed for marking up. Casual observation suggests that many articles are printed and then never looked at. A surprising number are never even picked up.

Non alpha numeric operating systems policy

Date: November 21, 2005

Subject: Use of Operating Systems with Non Alpha-numeric Characters

To: New Chemistry and Biochemistry Network Users

Background: Anytime a user of the Chemistry and Biochemistry network logs on to the system, a profile is retrieved from the network drives. This profile allows the network to "recognize" the user and to grant access to the appropriate resources as approved during the initial registration of the user. This process allows members of our Department great versatility to use computers throughout the building while maintaining the security necessary to keep unauthorized personnel from causing damage to our network infrastructure. Users also are able to have a similar interface regardless of where they log into the system. The profile must contain alpha-numeric characters unless it is stored on the user's personal computer. If it is stored on the individual's computer then the versatility of logging on from other computers in the department is lost. In addition, the interface with the network common drives cannot occur so the user does not have access to the common drives where many research groups save their data files and where the faculty store instructional programs for student use.

Recommendation: The Department's Computer Committee recommends that all users of the network use a licensed, alpha-numeric-based operating system on any computer being connected to the Department's network. Any exceptions to this policy must be approved by the CSR, Robert Paxman, with the following conditions being accepted by the user.

1. The operating system must be a licensed copy with full documentation to support ownership by the user.
2. The user understands that they will not be able to access the network except from their own personal computer.
3. The user understands that they will not be allowed access to the common drives to share research or instructional computer files.

All requests to use operating systems based on character sets that are not alpha-numerically based must submit a signed copy of this form to the CSR stating that they understand the restrictions imposed because of their request.

I request permission to use an operating system not based on alpha-numeric characters and understand the restrictions listed above.

____________________________ ____________________________________

Name Signature

____

Date

Department of Chemistry and Biochemistry
Security Policy

10. Introduction

With the recent growth in use of computer systems in teaching and research by students, staff and faculty, the need for security has become important. Our department has dealt with data loss, hijacking of department computers, hacking of computers, and theft of computer equipment. The only true security comes from locking computers in rooms, and allowing no access to them, and not connecting them to public networks. This is not an acceptable solution. The purpose of this policy is to balance the needs of computer security with the need of people to accomplish their work. The primary responsibility for security will always lie with computer users and their honesty and care in protecting equipment and information.

11. Physical Security

11.1. Server and infrastructure

11.1.1. The most basic and important equipment in the department are the server and network switches which OIT and the CSR office operate. Department servers hold important data, including confidential grades and other documents. Because of their importance, physical access to server equipment will be in a locked server room, which is keyed differently from the rest of the department. Key access to this room will be limited to the CSR office and necessary department officials.

11.1.2. Department data servers also need to be guaranteed during power surges and outages. An uninterruptible power supply (UPS) has been installed and connected to the backup generator power to provide this protection. CSR staff will identify key systems which need to be connected to this system.

11.1.3. Network switches are placed in wiring closets throughout the building. These closets are shared with network and phone equipment operated by OIT. Key access to these closets is described by the Joint Operation of Networking Agreement. Wiring equipment will be in self-contained rack systems (Locked?) Because of the difficulty in programming the switching equipment, UPS systems will be installed to protect from power surges and outages.

11.2. Faculty and Staff desktop computers

11.2.1. Access devices provided to faculty and staff are more difficult to secure. Computer users have the responsibility of making sure that office doors are locked to protect these computers. The department will provide locks for computer where necessary.

11.3. Faculty and Staff laptop computers

11.3.1. In many cases faculty and staff will find that laptop computers are necessary for their work. These mobile computers cannot easily be tied into the department password system, and thus require local passwords. The department will provide locks for computer where necessary.

11.4. Laboratory computers

11.4.1. Computers used in student offices and research laboratories are more difficult to secure. They are placed in public areas, and are accessed by a larger number of users. Physical security is provided by placing computers in rooms that can be locked. The department maintains a video surveillance system which can help. The department will provide locks for computer where necessary.

11.5. Student owned computers

11.5.1. Students are often bringing computers into the department as part of their work. They bear the primary responsibility for physical security of their computers, though the department maintains some lockable desk drawers which can be used for securing computers.

12. Access Security

12.1. Access to department of chemistry accounts

12.1.1. The CSR office provides a software system which allows access to department owned computers based on a single password. Faculty and staff are strongly encouraged to use this password system to provide access to computers. In cases where local password access is necessary, the primary computer user is responsible for controlling user access in accord with department of policies. The department maintains a database of chemistry computer user names and passwords for department work. This will provide access to all computer services provided by the department.

12.1.2. Faculty and staff working in department will be provided accounts on an open-ended basis.

12.1.3. Undergraduate and graduate research assistants will be provided with accounts as long as they are actively working in the department

12.1.4. Students who are enrolled in chemistry courses which require computer access will be provided with accounts for the length of time that they are enrolled in chemistry classes.

12.1.5. Accounts for visiting scientists, department visitors or other special cases will be coordinated through the CSR office and the department chair

12.1.5.1. Users are responsible for maintaining the security of their accounts, including securing their passwords. No chemistry users should share their accounts with other users.

12.2. Password policy

12.2.1. As BFW wrote it

12.3. End of life account policy

12.3.1. Students who are no longer enrolled in chemistry classes will automatically have their accounts suspended, and the data will be deleted after two semesters of inactivity.

12.3.2. Students and staff who have accounts in the department are responsible for visiting the CSR office to discuss their accounts upon leaving the department. Accounts will no longer be maintained six months after users leave the department.

12.4. Sharing of data

12.4.1. One important role of the network is to provide data portability in the department. In the past this has been accomplished by having large shared network file storage shares. The department now has a system which allows the creation of user groups which have private shared file areas. Users are encouraged to used these group areas as much as possible. The shared are will continue to exist, but files will be automatically deleted after a set time.

12.5. Wireless data

12.5.1. Limited to Chemistry users

12.5.2. Limit signal to Benson building

12.6. Connection of non-BYU computers to Chemistry network

12.6.1. Viruses and other security vulnerabilities have made operation of department computers more difficult. Computers which are brought into the department by users are inherently more difficulty to secure than department owned machines. Users who bring computer in need to make sure that all current operating system patches are installed, and that they have current virus protection software installed and updated.

13. Access to network from outside of department

13.1. Computer network attacks have become more common. Since it is difficult to guarantee that all computers on the department network are secure, the department will maintain a firewall computer which filters traffic from outside of the department. Deployment of this firewall will be coordinated with OIT as described in the Joint operating agreement. This firewall will block all incoming data ports for normal computers, including web servers, mail other connections. The CSR office will maintain servers for web, mail and other serviced which need to have outside network access, and will guarantee that these computers are maintained with the latest software patches and virus protection.

13.2. In order to keep sensitive data protected, department file servers will have no direct external access from outside of the chemistry department network.

13.3. In order to provide access to department computers from outside the department, the CSR office will maintain a virtual private network (VPN) server. All access to the chemistry network from outside the department will use this VPN. Department users will be given access to the VPN on an as needed basis by the CSR office.

14. Patch and Virus control policy

14.1. Server and Infrastructure

14.1.1. Constant changes in the security situation make it necessary to keep up with security patches and virus updates. In the case of servers this is especially important. CSR staff will monitor appropriate sources and install all security patches and virus detection files within 72 of being issued. They will also work with the computer committee in developing appropriate e-mail filters to minimize the impact of e-mail based viruses.

14.2. Access devices

14.2.1. Responsibility for application of necessary security patches or virus detection files belongs to the primary user of department computers. The CSR office will notify users within 24 hours of important security patches, and will provide support to users in applying those patches. Patches will be applied to all computers connected to the department network within 72 hours, or the CSR office is empowered to disconnect them from the network after proper notification.

14.2.2. c. Any computer found to contain virus files or has other security problems can be disconnected in order to maintain the security of the network. The CSR office will then work with the primary user to clear up the security problem

15. Backup Policy

15.1. Overview

15.1.1. Data files generated both in teaching and research are crucial to the functions of the department. As a department we need to make sure that all data is properly backed up in order to make sure that this data is not lost. The primary responsibility for this belongs with the user. Each person in the department can make sure that data is saved in multiple locations (such as on a local disk and on the department file server) so that the chances of loss are minimized. The department will also provide facilities to write data to a permanent media, such as a CD-ROM or DVD-ROM disk, so that individual users can make permanent copies of their files. The CSR office maintains department file servers for faculty, research and student needs. File space on this server will be made available for storage, and files stored will be backed up on a regular basis. Finally, a mechanism will be created for archiving important data.

15.2. Definitions

When developing policy for computer file backup, we will define two different types of backup.

a) Disaster Recovery

Disaster recovery is important when data is lost as a result of a hardware failure. The goal of this is to restore the lost data up to the point in time of the hardware failure.

b) Archiving

Archiving is important either when the data cannot be stored as normal files (for example because the files are too big) or when files have been accidentally deleted and need to be recovered. The goal here is to guarantee that important data is always available.

15.3. Desktop and Laptop computers

15.3.1. Given the rapid growth in the size of computer hard drives, backup media, such as tapes, have not kept pace with capacity. This makes it difficult to provide a simple backup procedure. In most cases the majority of data on a hard drive is programs and program data, which can easily be reinstalled in the case of a disaster, and which does not need to be archived. Computer users will be responsible for identifying what data on their computer need backing up, since they know best what files are irreplaceable. Users should keep copies of this data either in a permanent media, such as a CD-ROM or DVD-ROM, or on the department file server, or both. This data will then be quickly accessible in cases of local data loss. The CSR office will keep original media of software available so that a computer can be quickly rebuilt with necessary programs, and the data files copied back from the server or other media.

15.4. Department File Server

15.4.1. Given the importance of computer data, the department will provide a secure and fully backed up file server. This server will have sufficient performance and capacity to meet the needs of the department. This system will store all files in a redundant fashion, such as a RAID 5 array to make sure that data is not lost in the event of a disk failure. Backup of the server needs to be considered both from a disaster recovery and an archiving standpoint. The total amount of data stored on the server is large in comparison to any available archival system (in its current incarnation it would require 500 DVD-ROM disks to provide a backup for the entire array), so it is necessary to consider the importance of specific data. On the server it will be the responsibility for users to mark data directories as being necessary to archive or not. Data marked as needing to be archived will be copied to an external hard drive. Backup copies of server data will be made at least every 48 hours and copies will be kept for at least 7 days. A disk copy of data will be stored in the library vault every week, and a copy kept in the Church owned vault in Salt Lake City every month.

16. E-mail and IM

16.1. E-mail and instant messaging (IM) have become important teaching and research tools. Because of this, the department maintains an e-mail server for department use. As with all servers visible outside of the department, the CSR office will make sure that all unnecessary ports and services are turned off, and that all security patches are applied. Mail will be stored on a redundant disk array, and will be backed up according to the department backup policy.

16.2. Use of e-mail by users will subject to campus standards.

16.3. Although the University allows for personal and ecclesiastical use of computer resources, including their use in network communications, it expects such use to be minimal and should not occur under circumstances that interfere with University or personnel work responsibilities or that inappropriately consume finite resources (see Conflict of Interest and Conflict of Time Policy).

16.4. Use of computer resources for advertising, selling, and soliciting is prohibited without the prior written consent of the University. Any such uses must comply with the University's Advertising/Selling/Soliciting Policy.

16.5. E-mail in inherently insecure as a communications tool. Unauthorized users may be able to read electronic communications. Users should take appropriate precautions when sending sensitive information.

16.6. The department retains the right to monitor e-mail and IM traffic for inappropriate traffic. Any monitoring will be conducted by full-time staff in the CSR office, and must be approved by the department chairman.

16.7. The CSR office retains the right to filter incoming e-main and IM traffic for unrequested communications, or "spam", and computer viruses or worms. The department currently filters for .exe , .zip and other types attachments which are known to contain viruses.

17. Web access

17.1. The department is concerned with the access of inappropriate material, including pornography, in the department. The department maintains a computer system for scanning web page requests. These requests are compared to a list of key words and known sites to identify inappropriate requests. The CSR office will provide information from these scans to the department chairman who will decide on disciplinary actions

17.2. The CSR office and the computer committee will look at proxy servers which can stop requests to sites not considered appropriate to BYU’s mission.

18. Review of Security issues

18.1. The security situation changes constantly. The CSR office will keep up-to-date on current security concerns, and will present issues to the computer committee as warranted.

18.2. Committee review security policy every 6 months.

18.3. Where possible the CSR office will consult with the computer committee on changes in policy of operations necessary to react to respond to security concerns. If this is not possible, the CSR office can make necessary changes but will meet with the committee within 48 hours of the changes to discuss the need for the changes.

Information Security Policy

This set of guidelines on corporate information security comes to us from Henry Dumas, the IS manager at Hano Document Printers in Springfield, MA. We're presenting it here to serve as a framework for your own information security policy or to compare to the one your organization has on the books.

Dumas said that to ensure that employees understand the policy, the company provides a copy for each worker. Employees also attend a meeting to help them understand why the policy is so important to the company.

After reading the policy, workers sign a form acknowledging that they have read the policy and understand it. We've included that form in this download. To make sure that the business is following its own guidelines, the company conducts routine compliance audits.

Introduction

Computer information systems and networks are an integral part of business at Hano Document Printers. The company has made a substantial investment in human and financial resources to create these systems.

The enclosed policies and directives have been established in order to:

- Protect this investment.
- Safeguard the information contained within these systems.
- Reduce business and legal risk.
- Protect the good name of the company.

Violations

Violations may result in disciplinary action in accordance with company policy. Failure to observe these guidelines may result in disciplinary action by the company depending upon the type and severity of the violation, whether it causes any liability or loss to the company, and/or the presence of any repeated violation(s).

Administration

The information services manager (IS manager) is responsible for the administration of this policy.

Contents

The topics covered in this document include:

- Statement of responsibility
- The Internet and e-mail
- Computer viruses
- Access codes and passwords
- Physical security
- Copyrights and license agreements

Statement of responsibility

General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities.

Manager responsibilities

Managers and supervisors must:

Ensure that all appropriate personnel are aware of and comply with this policy.
Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

IS manager responsibilities

The IS manager must:

1. Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives.
2. Provide appropriate support and guidance to assist employees to fulfill their responsibilities under this directive.

The Internet and e-mail

The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide. One popular feature of the Internet is e-mail.

Policy

Access to the Internet is provided to employees for the benefit of Hano Document Printers and its customers. Employees are able to connect to a variety of business information resources around the world.

Conversely, the Internet is also replete with risks and inappropriate material. To ensure that all employees are responsible and productive Internet users and to protect the company’s interests, the following guidelines have been established for using the Internet and e-mail.

Acceptable use

Employees using the Internet are representing the company. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Using Web browsers to obtain business information from commercial Web sites.
- Accessing databases for information as needed.
- Using e-mail for business contacts.

Unacceptable use

Employees must not use the Internet for purposes that are illegal, unethical, harmful to the company, or nonproductive. Examples of unacceptable use are:

- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Broadcasting e-mail, i.e., sending the same message to more than 10 recipients or more than one distribution list.
- Conducting a personal business using company resources.
- Transmitting any content that is offensive, harassing, or fraudulent.

Downloads

File downloads from the Internet are <u>not</u> permitted unless specifically authorized in writing by the IS manager.

Employee responsibilities

An employee who uses the Internet or Internet e-mail shall:

1. Ensure that all communications are for professional reasons and that they do not interfere with his/her productivity.

2. Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet. All communications should have the employee's name attached.
3. Not transmit copyrighted materials without permission.
4. Know and abide by all applicable Hano policies dealing with security and confidentiality of company records.
5. Run a virus scan on any executable file(s) received through the Internet.
6. Avoid transmission of nonpublic customer information. If it is necessary to transmit nonpublic information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.

Copyrights

Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the company and/or legal action by the copyright owner.

Monitoring

All messages created, sent, or retrieved over the Internet are the property of the company and *may be regarded as public information*. Hano Document Printers reserves the right to access the contents of any messages sent over its facilities if the company believes, in its sole judgment, that it has a business need to do so.

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. **This means don't put anything into your e-mail messages that you wouldn't want to see on the front page of the newspaper or be required to explain in a court of law.**

Computer viruses

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of corporate resources.

Background

It is important to know that:

- Computer viruses are much easier to prevent than to cure.
- Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

IS responsibilities

IS shall:

1. Install and maintain appropriate antivirus software on all computers.
2. Respond to all virus attacks, destroy any virus detected, and document each incident.

Employee responsibilities

These directives apply to all employees:

1. Employees shall not knowingly introduce a computer virus into company computers.
2. Employees shall not load diskettes of unknown origin.
3. Incoming diskettes shall be scanned for viruses before they are read.
4. Any associate who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and call the IS manager.

Access codes and passwords

The confidentiality and integrity of data stored on company computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

IS responsibilities

The IS manager shall be responsible for the administration of access controls to all company computer systems. The IS manager will process adds, deletions, and changes upon receipt of a written request from the end user's supervisor.

Deletions may be processed by an oral request prior to reception of the written request The IS manager will maintain a list of administrative access codes and passwords and keep this list in a secure area.

Employee responsibilities

Each employee:

1. Shall be responsible for all computer transactions that are made with his/her User ID and password.
2. Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained.
3. Will change passwords at least every 90 days.
4. Should use passwords that will not be easily guessed by others.
5. Should log out when leaving a workstation for an extended period.

Supervisor's responsibility

Managers and supervisors should notify the IS manager promptly whenever an employee leaves the company or transfers to another department so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

Human resources responsibility

The Personnel Department will notify MIS monthly of associate transfers and terminations. Involuntary terminations must be reported concurrent with the termination.

Physical security

It is company policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

Employee responsibilities

The directives below apply to all employees:

1. Diskettes should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.
2. Diskettes should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
3. Critical computer equipment, e.g., file servers, must be protected by an uninterruptible power supply (UPS). Other computer equipment should be protected by a surge suppressor.
4. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
5. Since the IS manager is responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities. This does not apply to temporary moves of portable computers for which an initial connection has been set up by IS.

6. Employees shall not take shared portable equipment such as laptop computers out of the plant without the informed consent of their department manager. Informed consent means that the manager knows what equipment is leaving, what data is on it, and for what purpose it will be used.
7. Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.

Copyrights and license agreements

It is Hano’s policy to comply with all laws regarding intellectual property.

Legal reference

Hano and its employees are legally bound to comply with the Federal Copyright Act (Title 17 of the U. S. Code) and all proprietary software license agreements. Noncompliance can expose Hano and the responsible employee(s) to civil and/or criminal penalties.

Scope

This directive applies to all software that is owned by Hano, licensed to Hano, or developed using Hano resources by employees or vendors.

IS responsibilities

The IS manager will:

1. Maintain records of software licenses owned by Hano.
2. Periodically (at least annually) scan company computers to verify that only authorized software is installed.

Employee responsibilities

Employees shall not:

1. Install software unless authorized by IS. Only software that is licensed to or owned by Hano is to be installed on Hano computers.
2. Copy software unless authorized by IS.
3. Download software unless authorized by IS.

Civil penalties

Violations of copyright law expose the company and the responsible employee(s) to the following civil penalties:

- Liability for damages suffered by the copyright owner
- Profits that are attributable to the copying
- Fines up to $100,000 for each illegal copy

Criminal penalties

Violations of copyright law that are committed “willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b)),” expose the company and the employee(s) responsible to the following criminal penalties:

- Fines up to $250,000 for each illegal copy
- Jail terms of up to five years

Acknowledgment of Information Security Policy

This form is used to acknowledge receipt of, and compliance with, the Hano Document Printers Information Security Policy.

Procedure

Complete the following steps:

1. Read the Information Security Policy.
2. Sign and date in the spaces provided below.
3. Return this page only to the information services manager.

Signature

By signing below, I agree to the following terms:

i. I have received and read a copy of the “Information Security Policy” and understand the same;

ii. I understand and agree that any computers, software, and storage media provided to me by the company contains proprietary and confidential information about Hano Document Printers and its customers or its vendors, and that this is and remains the property of the company at all times;

iii. I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at Hano Document Printers), otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;

iv. I agree that, if I leave Hano Document Printers for any reason, I shall immediately return to the company the original and copies of any and all software, computer materials, or computer equipment that I may have received from the company that is either in my possession or otherwise directly or indirectly under my control.

Employee signature: ________________________________

Employee name: ________________________________

Date: ________________________________

Department: ________________________________

Security resource list for administrators

As new and more dangerous network security threats proliferate, administrators need to know as much as possible about these threats and about the vulnerabilities that leave networks open to attack. The better armed net admins are with knowledge of threats and security measures, the better able they'll be to secure their networks and fend off attacks.

The following links are to Web sites that can offer valuable information about securing your networks, including updates on new threats and vulnerabilities and how to deal with them, as well as downloads of utilities and information about products that can help you secure your networks.

Many of the links in this document were provided by Global Knowledge in Network Security I courseware, David Ford, course director.

Security organization and information sites

SecurityPortal (http://www.securityportal.com)

SecurityPortal offers various security information and services. The site is currently down for upgrades, and users are being redirected to security solution provider RedSiren Technologies.

Microsoft Security (http://www.microsoft.com/security)

Yes, Microsoft's Web site offers important tips and other information to help you secure your network. In addition to valuable information, Microsoft provides security services.

TruSecure Corp (http://www.trusecure.com)

TruSecure is a security solutions provider that also certifies security products. TruSecure has established the TruSecure ICSA Certified Security Associate (T.I.C.S.A.) certification for IT professionals.

U.S. Dept. of Justice CCIPS (http://www.cybercrime.gov/)

The Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice Web site presents detailed information about policy regarding computer crime, procedures for reporting computer crime, and news relating to computer crime cases.

National Infrastructure Protection Center (NIPC) (http://www.nipc.gov)

The NIPC assesses and investigates threats to critical infrastructures and provides warnings about threats and vulnerabilities.

NTBugtraq (http://www.ntbugtraq.com)

NTBugtraq is a mailing list devoted to security exploits and bugs in Windows NT, Windows 2000, and Windows XP.

SecurityFocus Online (http://online.securityfocus.com/cgi-bin/sfonline/forums.pl)

SecurityFocus is a collection of security-related mailing lists. You can subscribe to the newsletter, which offers information about exploits, vulnerabilities, and threats, and you can take advantage of the mailing list to solicit information from members.

Computer Incident Advisory Capability (CIAC) (http://www.ciac.org/ciac/)

The U.S. Department of Energy's CIAC Web site offers news about new computer threats, hoaxes, and vulnerabilities, along with procedures for reporting incidents such as network attacks.

Forum of Incident Response and Security Teams (FIRST) (http://www.first.org)

FIRST is an international coalition formed to share information about network security threats and to work out responses to incidents. You can sign up for mailing lists and become a member. The annual membership fee is $550.00. FIRST holds an annual forum to discuss security issues.

Computer Emergency Response Team Coordination Center (CERT/CC) (http://www.cert.org)

CERT/CC is a center that specializes in Internet security issues at Carnegie Mellon's Software Engineering Institute. At its Web site, you'll find information about Internet vulnerabilities, security alerts, and information about fixing vulnerabilities.

Common Vulnerabilities and Exposures (CVE) (http://www.cve.mitre.org/)

CVE is a dictionary of information security vulnerability and exposure terms.

The National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) (http://csrc.ncsl.nist.gov)

The CSRC is the Web site for the Computer Security Division (CSD) of the NIST's Information Technology Laboratory. The CSD's mission is to research and raise awareness of new IT vulnerabilities and to develop cost-effective security measures.

Information Systems Security Association (ISSA) (http://www.issa.org)

ISSA is an international organization of IT security professionals established to educate its members about security issues and measures and to publish the findings of its forums on security-related issues.

International Information Systems Security Certification Consortium (ISC2) (http://www.isc2.org)

The ISC2 Web site provides information about becoming a Certified Information Systems Security Professional (CISSP).

High Technology Crime Investigation Association (HTCIA) (http://www.htcia.org)

The HTCIA is an international organization established to set standards for investigating technology crimes.

Center for Education and Research in Information Assurance and Security (CERIAS) (http://www.cerias.purdue.edu/)

CERIAS is Purdue University's center for research on information security issues. It offers a wealth of information on vulnerabilities and threats.

Security product links

The following list represents products that can help you better secure your network. This is not an endorsement of the products but a list of those that are well known.

Firewalls

- Check Point FireWall-1 (http://www.checkpoint.com/products/protect/index.html)
- Cisco Secure PIX 500 series (http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/)
- Symantec VelociRaptor (http://enterprisesecurity.symantec.com/products/products.cfm?productID=49)
- Secure Computing's Sidewinder (http://www.securecomputing.com/index.cfm?skey=232)
- BorderWare Firewall Server (http://www.borderware.com/)
- Elron Software's Internet Manager (IM) Firewall (http://www.elronsw.com/productfamily/firewall.shtml)
- CyberGuard LX, FS, KS, and SL VPN/firewall appliances (http://www.cyberguard.com/SOLUTIONS/product_intro.cfm)
- WatchGuard Firebox series (http://www.watchguard.com/products/wgls.asp)
- SonicWALL appliances (http://www.sonicwall.com/)

Be sure to check out products from Network Associates (http://www.networkassociates.com) as well.

Intrusion detection systems (IDS)

- Symantec Intruder Alert (acquired with Axent) (http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=48&PID=11649525&EID=0)
- Symantec NetProwler (acquired with Axent) (http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=50&PID=11649525&EID=0)

- Cisco IDS series (http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/)
- Entercept Security Technologies' Entercept (http://www.clicknet.com/products/entercept/)
- Internet Security Systems RealSecure Network Sensor (http://www.iss.net/products_services/enterprise_protection/rsnetwork/sensor.php)
- NFR Security's Network Intrusion Detection (NID) (http://www.nfr.net/products/)
- Intrusion Inc.'s SecureNet products (http://www.intrusion.com/products/productcategory.asp?lngCatId=4)
- Tripwire, Inc.'s intrusion detection and data integrity products (http://www.tripwire.com/)
- Psionic's TriSentry Suite (freeware) (http://www.psionic.com/products/index.html)

Scanners (vulnerability assessment and auditing tools)

- Symantec NetRecon (http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=46&PID=11649525&EID=0)
- Internet Security Systems (ISS) scanning products (http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/index.php)
- Cisco Secure Scanner (http://www.cisco.com/warp/public/cc/pd/sqsw/nesn/)
- McAfee CyberCop ASaP (http://www.mcafeeb2b.com/services/cybercop-asap.asp)
- NetIQ's Security Analyzer (http://www.netiq.com/solutions/security/default.asp)
- Nessus (freeware) (http://www.nessus.org)
- HP Webenforcer (http://www.hp.com/security/products/webenforcer/)

Authentication

- Netegrity SiteMinder (http://www.netegrity.com/products/?leveltwo=SiteMinder)
- IBM Tivoli Access Manager (http://www.tivoli.com/products/solutions/security/access.html)
- *RedCreek Ravlin series (http://www.redcreek.com/products/index.html)
- *SonicWALL Authentication Service (http://www.sonicwall.com/authentication-service/solutions.html)
- RSA SecurID (http://www.rsasecurity.com/products/securid/index.html)
- Entrust GetAccess (http://www.entrust.com/getaccess/index.htm)
- Funk Software's Steel-Belted Radius (http://www.funk.com/radius/enterprise/enterprise_radius.asp)
- ActivCard (http://www.activcard.com)
- CRYPTOCard CRYPTOLogon, CRYPTOWeb, and CRYPTOAdmin (http://www.cryptocard.com/index.cfm?CID=8&NAVCID=8&PageName=Solutions%20for%20your%20Network)
- Gemplus GemSAFE products (http://www.gemplus.com/index.html)
- Vasco Digipass series (http://www.vasco.com/products/range.html?VSID=5e65eb874a61e5e501501b1bbdaf9f53#Digipass)

*Red Creek acquired Internet Dynamics, which offered Conclave, and was later acquired by SonicWALL. Thus, RedCreek and Internet Dynamics products may be pulled under the SonicWALL umbrella.

Antivirus and content filtering software

- Trend Micro antivirus products (http://www.antivirus.com/products/)
- Symantec (Norton) AntiVirus Enterprise Edition (http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=64&PID=1117941&EID=0)
- McAfee VirusScan (http://www.mcafee.com/myapps/default.asp?)
- SonicWALL Complete Anti-Virus (http://www.sonicwall.com/anti-virus/index.html)
- SurfControl SuperScout (http://www.surfcontrol.com/business/products/)
- GFI Mail essentials (http://www.gfifax.com/mes/index.html)
- Tumbleweed's Secure Mail (http://www.tumbleweed.com/en/products/solutions/protect_enterprise/mail.html)
- Elron's Internet Manager (http://www.elronsw.com)

Hacker sites

TechRepublic
Real World. Real Time. Real IT.

Security resource list

Hacker sites offer good information about the latest threats and newly discovered vulnerabilities. They also offer freeware downloads of scanners and other utilities that you can use to identify vulnerabilities—so that you can see what hackers see. Don’t download and install anything without scanning it first, though. While these sites can help you beef up your security arsenal, you should still proceed with caution.

AntiOnline (http://www.antionline.com/index.php)

For information and news about vulnerabilities and threats, AntiOnline is one of the best of the hacker sites. It includes a wealth of downloads from antivirus programs to exploits and scanners. AntiOnline also offers an extensive list of links divided into a number of categories so you can find more sites about security and hacking.

2600 Magazine The Hacker Quarterly home page (http://www.2600.com)

This site offers news and information from the hacker community.

Phrack Magazine (http://www.phrack.org)

Here's another hacker publication offering news and information.

Hackers.com (http://www.hackers.com)

Hackers.com offers information about vulnerabilities, threats, and exploits, as well as advice on securing networks.

L0pht Heavy Industries at @Stake (http://www.atstake.com/research/redirect.html)

This site features information about vulnerabilities and threats, along with downloads for auditing network security, including LC4, a password auditing and recovery application.

Cult of the Dead Cow (http://www.cultdeadcow.com)

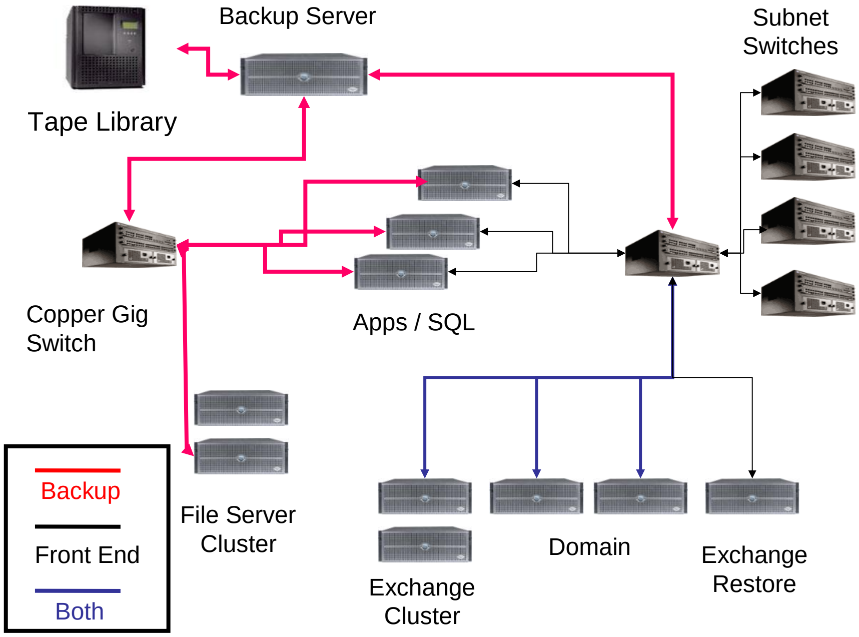
Cult of the Dead Cow offers news and comments about issues of hacking and security. You can also download files from the site, including Back Orifice and Whisker.

Def Con (http://www.defcon.org)

This Web site promotes the annual hacker convention and offers links to a variety of downloads, including cracks, scanners, and other tools.

Backup network solution

Detailed specs for a build-your-own backup network solution



Backup network copper Gig switch

(1) Foundry Server Iron II—Layer 2/3 Switch

(2) 8 Port Copper Gig Blades

(1) 24 Port 10/100 Blade

*Note: Addressed as non-routed Class C Network 192.168.x.x

Backup network interface cards for servers

Broadcom copper Gigabit

3Com—10/100 3c980C

Backup server

Dell Power Edge 2450

933 MHz

512 MB memory

Intel Pro 1000 (Fiber) Gigabit NIC (Front-end Network)

Broadcom copper Gigabit NIC (Backup Network)

*Note: This system cannot use DNS or WINS servers. All name resolution is done via HOSTS and LMHOSTS files.

Backup network solution

Tape library

Dell Power Vault 130T

4 DLT 7000 drives and 28 available slots

Backup software

Veritas Backup Exec Version 8.6

Datacenter Server Edition

Open File Option

Library Expansion Option

Remote Agent for Windows

Agent for Microsoft Exchange

*Note: Veritas NetBackup met more requirements but was too expensive.

File server cluster

(2) Dell Power Edge 6450

Quad XEON 700MHz 512MBCACHE

2 GB RAM

18 GB RAID1—System Partitions

Shared Disks

Dell Power Vault 200s 100GB Array

Dell Power Edge SE300 Cluster Configuration supporting up to four Dell Power Vault 2xx Disk Arrays. Cluster diagram shown below. More details are available from Dell.

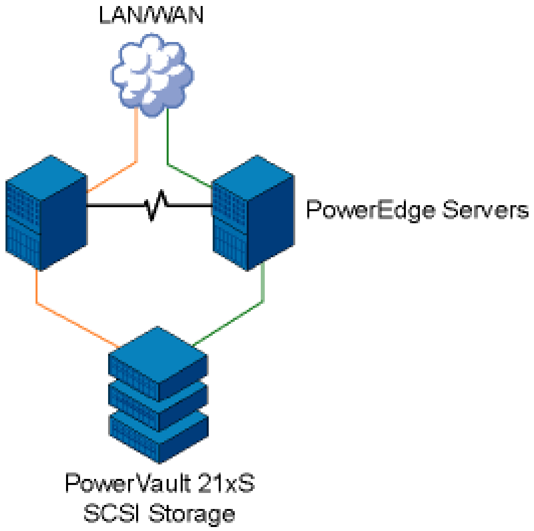


Figure reproduced from Dell.com.

Special notes:

Exchange environment considerations

After attempts at setting up the cluster as Active/Active were not successful, the cluster was set up as an Active/Failover application server cluster. The virtual application server is created on the public network only. The Veritas backup agent requires this resource to properly back up the Exchange databases. For this reason, backup of our Exchange server cluster could only be accomplished on the public network.

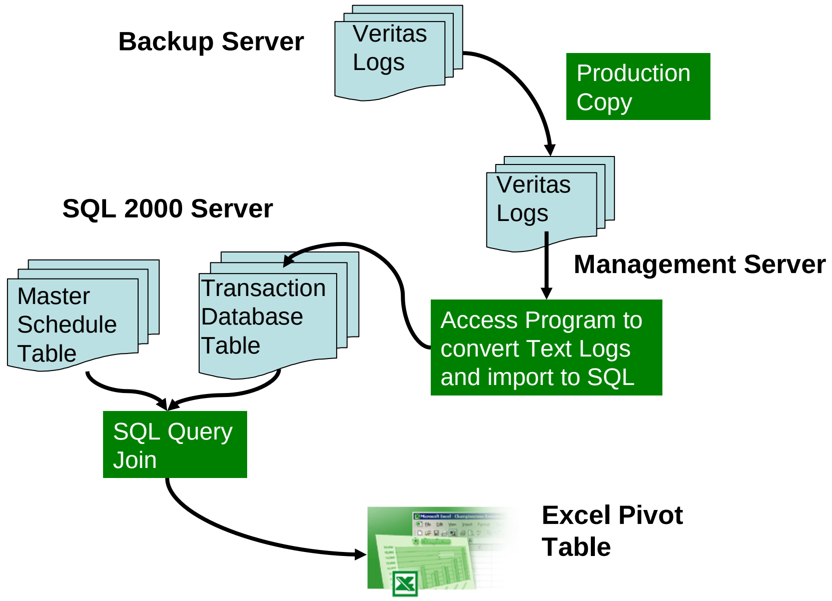
The backup server has Ethernet interfaces on both networks to work around this issue. A separate Exchange restore server was needed on the front-end network, connected to the Windows 2000 Domain with its own DLT tape drive.

Domain controller consideration

DNS and WINS services run on the domain controllers in this environment. If you were to multi-home this server, clients could receive addressed requests for resources on the wrong network. For this reason, we backed up the domain controllers on the public network.

Backup network reporting system

Basic application architecture



Application process

- Set up an automated procedure to copy the backup logs from the backup server to a central location on the front-end network.
- Write programs to read the logs and load pertinent information into the SQL tables creating needed new fields.
- Establish success values:
  - Verified
  - Backed up
  - Failed
  - Not Started
- Establish percent completed
  - Number of files needed to be backed up
  - Number of files actually backed up
- Establish major IT service/application linkage
  - Needed to link to IT reporting system
  - Needed to show backup and restore performance by major service, e.g., file server by location, sales intranet, etc.

- Update the master-reporting database weekly, so the information is available on Monday mornings.
- Integrate the information into the master IT reporting system.

System components

- Microsoft SQL Server 2000
- Microsoft Access Programming Language
- Microsoft Excel Pivot Tables
- Server scheduling and coping of the Veritas Log Files
- Veritas Enterprise Backup Software

Basic Veritas SQL table contents

Name	Type	Size
Job ID	Long integer	4
Description of the backup job	Text	100
Backup started	Date/Time	8
Backup ended	Date/Time	8
Number of files	Single	4
Size of files	Long integer	4
Verify started	Date/Time	8
Verify ended	Date/Time	8
Files different	Long integer	4
Backup date	Date/Time	8

Sample code used to read and convert Veritas logs

```
Function JobInfo(FileName As String, JobId As Integer)

 ‘Define variables for storing the data items read from the text file
 ‘Open FileName  For Reading
 ‘Read each line one at a time
’Get Detail Information For All Backups In the Log
```

What you read would depend on the backup program that produced the log and the fields that needed to be read. In our case, the field we were looking for in the example below (Backup started on) was 17 characters long. So we started from 19 spaces, took the string, and passed it to the DetailDate function. This function converted the string into an actual database storable valid date.

```
If Left(InputData, 17) = "Backup started on" Then
          BackupStarted = DetailDate(Trim(Mid(InputData, 19, Len(InputData))))
End If
```

When all the fields are read, insert the record into the database.

```
’Reset All the variables
```

Once this is done, you would need to open the file again to read the verify operation. Some sample code is below.

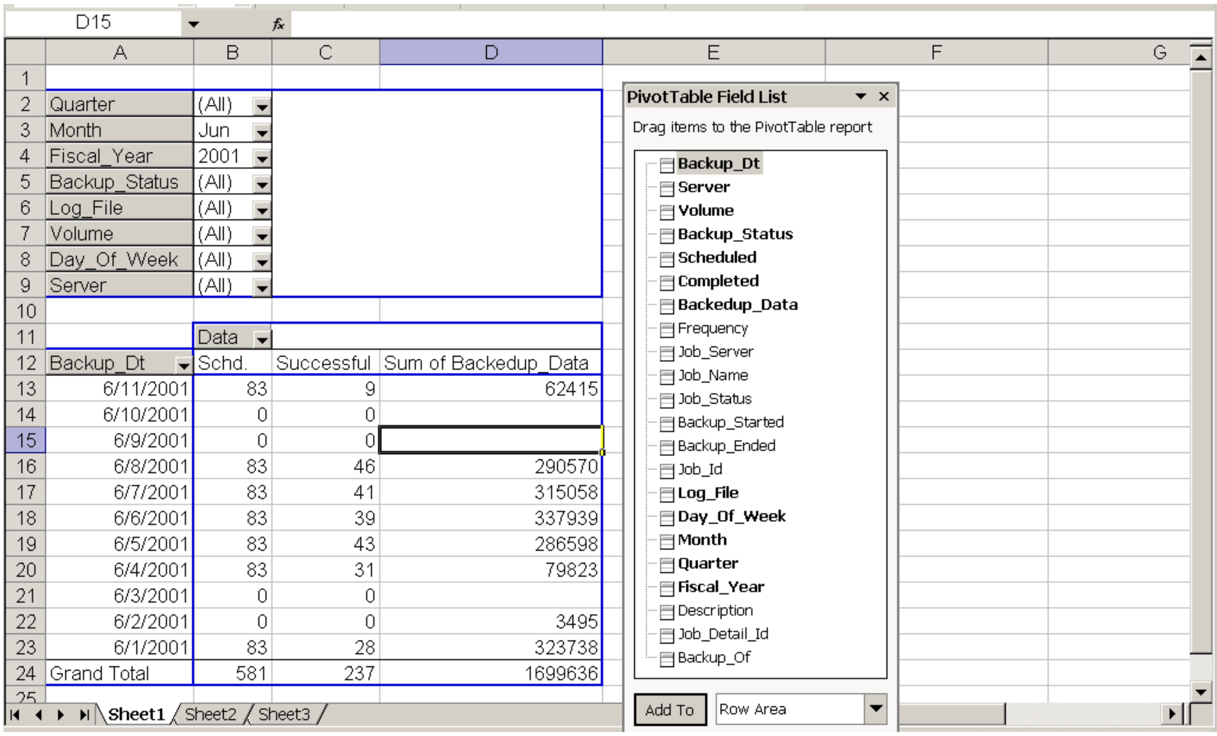
```
’ Get Detail Information For All Verifications In the Log
    ProcessVerify = "N"
    Open FileName For Input As #1
    Do While Not EOF(1)             ' Check for end of file.
        Line Input #1, InputData    ' Read line of data.
        'Debug.Print InputData       ' Print to the Immediate window.

    'Skip All Lines till the Verify operation Begins
        If Left(InputData, 22) = "Job Operation - Verify" Then
            ProcessVerify = "Y"
        End If
```

Then you would need to update the back up line corresponding the verification just read.

```
End Function
Function DetailDate(DateStr As String)

Dim DateEndPos As Integer
Dim strDatePart As String
Dim strTime As String
Dim TimePos As Integer
Dim FormatDateStr As String
    'Friday, April 13, 2001 at 7:06:47 PM
    'DateStr = "4/13/2001 at 7:07:29 PM"

'Get Date Part
    DateEndPos = InStr(1, DateStr, "at", vbTextCompare)
    strDatePart = Trim(Left(DateStr, DateEndPos - 1))
'Get Time
    'strTime = Trim(Mid(DateStr, (DateEndPos + 2), Len(DateStr)))
    strTime = Trim(Mid(DateStr, (DateEndPos + 2), (Len(DateStr) - (DateEndPos + 2))))

    FormatDateStr = strDatePart & " " & strTime
    DetailDate = FormatDateStr

End Function
```

Demo pivot table screen capture

The screen capture below highlights a sample pivot table that shows original and created fields. As you can see, information can be looked at from many different views.



Quarter	(All)
Month	Jun
Fiscal_Year	2001
Backup_Status	(All)
Log_File	(All)
Volume	(All)
Day_Of_Week	(All)
Server	(All)

	Data		
Backup_Dt	Schd.	Successful	Sum of Backedup_Data
6/11/2001	83	9	62415
6/10/2001	0	0	
6/9/2001	0	0	
6/8/2001	83	46	290570
6/7/2001	83	41	315058
6/6/2001	83	39	337939
6/5/2001	83	43	286598
6/4/2001	83	31	79823
6/3/2001	0	0	
6/2/2001	0	0	3495
6/1/2001	83	28	323738
Grand Total	581	237	1699636

Computer hardware inventory list

I've always believed that the first step to troubleshooting a PC, or any machine for that matter, is to know the equipment you're dealing with. While this sounds like a simple concept, I can't tell you how many times I've been confronted with a video adapter, sound card, motherboard, or other peripheral device that had no markings to identify the manufacturer or model. Such confusion can add minutes, if not hours, to the time it takes to resolve a problem—especially if you're downloading new drivers. To help you avoid issues like these, I've developed a computer hardware inventory list, which you'll find on the next page.

This list allows any tech, even one that's unfamiliar with the PC, to easily determine the make and model of the computer's essential components. I designed the form to be used in two ways. You can print the blank form and then fill in the necessary fields by hand, or you can open and complete the form in Microsoft Word using the drop-down menus and typing in the necessary information. To use the drop-down menus, you will need to protect the document first. To do this, click Tools | Protect Document, select Forms from the Protect Document pop-up window, and click OK.

The list includes fields for the following computer components:

- CPU
- Motherboard
- RAM
- Hard drive
- Power supply
- Hard drive 2
- Sound card
- Video card
- CD-R/RW
- DVD
- Modem
- NIC
- Other cards

Once you've completed the form, simply tape it inside the computer's case. Be sure to keep it out of the way of any ventilation holes, heat sinks, fans, or other moving parts; you don't want a loose piece of paper flapping around inside the PC. If you really want to get fancy, you could attach an antistatic bag inside the computer case and place the form within the bag.

Computer hardware inventory list

COMPONENT	DESCRIPTION (Include brand and model number.)
CPU	
Motherboard	
RAM	
Hard drive	
Choose one	
Choose one	
Choose one	
Choose one	
Choose one	
Choose one	
Choose one	
Choose one	
Choose one	

TechRepublic Real World. Real Time. Real IT.

Requesting dial-up access

Standard procedure for requesting dial-up access

	MANUAL				
SUBJECT Dial-up Account Policies and Procedures	NUMBER 1	REV 3	EFFECTIVE DATE	PAGE 1	OF 2
	SUPERSEDES	PREPARED BY		APPROVED BY	

1.0 Purpose:

It is the purpose of this Standard Procedure to identify the process of requesting and administering company-owned Internet access dial-up accounts.

2.0 Policy:

The Information Technology Department has purchased several Internet dial-up accounts for temporary use by company employees. Please note: There are a number of company employees who have permanent dial-up accounts as well. The purpose of the temporary dial-up account is to provide temporary Internet access to approved personnel who are conducting company business where connection to the corporate (Local Area Network) LAN is not available. The company-owned dial-up accounts are authorized for use by company employees on company-owned computers for conducting official company business. Company owned dial-up accounts will not be authorized for privately owned computers or for leisure activities.

> 2.1 All company supervisors, managers, and directors may request the use of a dial-up account on their own authority. All other company employees may request use of a dial-up account with the written approval of their supervisor, manager, or director.

3.0 Procedure:

When requesting the use of a dial-up account, the requester will contact the Information Technology Help Desk at (xxx)-xxx-xxxx. All requests should be made at least five business days before access is needed to ensure access availability. Exceptions can be made in some instances, on a case-by-case basis.

> 3.1 Dial-up access will be granted for a maximum of 10 business days. Exceptions can be made in some instances, on a case-by-case basis. At the end of 10 business days, access will automatically be terminated. It is the responsibility of the customer to request an extension, if required.

4.0 The help desk analyst on call will create a trouble-ticket documenting the request, and assign it to the next analyst in the queue.

5.0 The analyst on call will:

5.1 Determine if the requester is a company supervisor, manager, director, or other employee.

5.2 E-mail the appropriate document to the requester for signature, or have the requestor come to the help desk to pick up the document if e-mail is not an option. Blank documents will be located in a folder at the help desk entrance. The customer will sign the document and drop it in the drop box. There will be no need for the customer to interact with the help desk staff.

The help desk staff will make a note in the requester's trouble-ticket indicating that they have turned in the appropriate, signed form.

The form will be kept on file with the help desk supervisor for 12 months.

Note: If the requestor is not a supervisor, manager, or director, he or she must obtain a signature from the appropriate supervisor before access will be activated.

5.3 Indicate in the worklog the date that the customer wants to have dial-up access activated and the termination date.

The analyst on call will confirm the dial-up access start and end date with the customer, and make a note on the electronic calendar to activate access and terminate access on the appropriate dates. In addition, the analyst on call will check for account availability in the "Resource" feature of Outlook Calendar. The analyst on call will also obtain a password the requestor would like to use to access the temporary account, and put it in the requestor's trouble-ticket worklog. The password must consist of at least six letters and/or numbers. Characters, such as @!#&%$, are not acceptable. Customers should not give the help desk staff their domain password to use for this temporary account. The analyst on call will go to the EarthLink Web site at http://support.earthlink.net/support/MYACCT/index.jsp, 24 hours before the requestor requires access and change the account password to the password given by the customer. The day after the designated deactivation date, the analyst on call will go back to the EarthLink Web site and reset the password to one that only key IT staff will be privy to. Each time the dial-up account is activated for a customer, the account password will be changed to one chosen by the customer. When the account is deactivated, the password will be changed to a specified IT-established password.

Note: The CIO, prior to implementation, must approve changes to any portion of this standard operating procedure.

XXXXXXX

Information Technology CIO

Develop an effective disaster recovery plan

By Rick Schiesser

During the mid- and late 1990s, I managed the main IT infrastructure for a major motion picture studio in Beverly Hills, California. Just prior to my hiring, an event drastically changed the corporation's thinking about disaster recovery, and I was asked to develop a disaster recovery program of major proportions.

Two of this studio's most critical applications were just coming online and were being run on IBM AS/400 midrange processors. One of the applications involved the scheduling of broadcast times for programs and commercials for the company's new premier cable television channel. The other application managed the production, distribution, and accounting of domestic entertainment videos, laser discs, and interactive games. The company had recently migrated the development and production versions of these applications onto two more advanced models of the IBM AS/400—9406-level machines utilizing reduced instruction set computing (RISC) technology.

During the development of these applications, we began initial discussions about developing a disaster recovery plan for these AS/400s and their critical applications. In February 1995, the effort got a major jumpstart from an unlikely source. A distribution transformer that powered the AS/400 computer room from outside the building short-circuited and exploded. The damage was so extensive that repairs were estimated to take up to five days. With no formal recovery plan yet in place, IT personnel, suppliers, and customers all scurried to minimize the impact of the outage.

With the help of one of the company's key vendors, we quickly identified and activated a makeshift disaster recovery site located 40 miles away. Within 24 hours, the studio's AS/400 operating systems, application software, and databases were all restored and operational. This makeshift solution met most of the critical needs of the AS/400 customers during the six days that it eventually took to replace the failed transformer.

Three important lessons learned

This incident accelerated the development of a formal disaster recovery plan. It also underscored three important points about recovering from a disaster. The first point is that there are noteworthy differences between the concept of disaster recovery and that of business resumption. I'm defining business resumption as the ability to perform critical department processes as soon as possible after the initial outage. Full recovery from the disaster usually occurs many days after the start of the business resumption process.

In this case, we restored most of the company operations affected by the outage in less than a day after the transformer exploded. It took nearly four days to replace all the damaged electrical equipment and another two days to restore operations back to their normal state. Distinguishing between these two concepts helped during the planning process for the formal disaster recovery program—it let us focus on business resumption in meetings with key customers, while we focused on disaster recovery with key suppliers.

The second point is that most computer center outages are caused by relatively small, localized incidents like broken water mains, fires, smoke damage, or electrical equipment failures—not the flash floods, powerful hurricanes, or devastating earthquakes frequently highlighted in the media.

This isn't to say that you shouldn't be prepared for such a major disaster. Infrastructures that plan and test recovery strategies for smaller incidents are usually well on their way to developing a program to handle any size of calamity. While major calamities do occur, they are far less likely and are often overshadowed by the more widespread effects of the disaster on the community. What usually makes a localized computer center disaster so challenging is that the rest of the company is normally operational and desperately in need of the computer center services that have been disrupted.

The third point is that this extended outage prompted executive management to make a firm commitment to a formal disaster recovery plan. In many ways disaster recovery is like an insurance policy: You don't really need it until you really need it. This commitment was the first important step toward developing an effective disaster recovery process. A comprehensive program requires hardware, software, budget, and the time and efforts of knowledgeable personnel. The support of executive management is necessary to make these resources available.

Steps to developing an effective disaster recovery process

There are 10 steps to developing an effective disaster recovery process.

1. Obtain executive support. Executive support, particularly in the form of an executive sponsor, is necessary for developing a truly robust disaster recovery process. You need funding approval from senior management for the resources you need in order to design and maintain an effective disaster recovery program.

Another reason this support is important is that managers are typically the first to be notified when a disaster occurs. This sets off a chain of events involving management decisions about deploying the IT recovery team, declaring an emergency to the disaster recovery service provider, notifying facilities and physical security, and taking whatever emergency preparedness actions may be necessary. By involving management early in the design process, you secure their emotional and financial buy-in, thus increasing the likelihood that management will understand and fulfill its role in the disaster recovery process.

The executive sponsor has several other responsibilities. One is selecting a process owner. Another is getting the support of other managers to ensure that participants are properly chosen and committed to the program. These other managers may be direct reports, peers within IT, or, in the case of facilities, outside of IT. Finally, the executive sponsor needs to demonstrate ongoing support by requesting and reviewing frequent progress reports, offering suggestions for improvement, questioning unclear elements of the plan, and resolving issues of conflict.

2. Select a process owner. The process owner is the most important person in the disaster recovery process because of the many key roles he or she plays. The process owner must assemble and lead the cross-functional team in preparing the business impact analysis, identifying and prioritizing requirements, developing business continuity strategies, selecting an outside service provider, and conducting realistic tests of the process. The process owner should exhibit several key attributes and be selected very carefully. Potential candidates include an operations supervisor, the data center manager, and even the infrastructure manager.

3. Assemble a cross-functional team. The process owner must assemble representatives from appropriate departments into a cross-functional design team. Departments typically represented on this team include computer operations, applications development, server and systems administration, facilities, key customer departments, data security, physical security, and network operations. This team will work on requirements, conduct a business impact analysis, select an outside service provider, design the final overall recovery process, identify members of the recovery team, conduct tests of the recovery process, and document the plan.

4. Conduct a business impact analysis. Even the most thorough disaster recovery plan won’t be able to justify the expense of including every business process and application in the recovery. It’s important to inventory and prioritize critical business processes for the entire company. Key IT customers should help the process owner coordinate this effort to ensure that all critical processes are included. Processes that need to be resumed within 24 hours to prevent serious business impact, such as loss of revenue or major impact to customers, are rated as an A priority. Those processes that need to be resumed within 72 hours are rated as a B, and those that can take more than 72 hours are rated C. These identifications and prioritizations will be used to propose business continuity strategies.

5. Identify and prioritize requirements. One of the cross-functional team’s first activities is to identify the requirements for each process, such as business, technical, and logistical requirements. Business requirements include defining the specific criteria for declaring a disaster and determining which processes are to be recovered and in what time frames. Technical requirements include what type of platforms will be eligible as recovery devices for servers, disks, and desktops, and how much bandwidth will be needed. Logistical requirements include the amount of time allowed to declare a disaster and transportation arrangements at both the disaster site and the recovery site.

6. Assess possible business continuity strategies. Based on the business impact analysis and the list of prioritized requirements, the cross-functional team should propose and assess several alternative business continuity strategies. These will likely include alternative remote sites within the company and geographic hot sites supplied by an outside provider.

7. Choose participants and clarify their roles for the recovery team. The cross-functional team chooses the individuals who will participate in the recovery activities after any declared disaster. The recovery team may be similar to the cross-functional team but should not be identical. Additional members should include the executive sponsor, key customer representatives, and representatives from any outside service providers. Once the recovery team is selected, it's imperative that each individual's role and responsibility be clearly defined, documented, and communicated.

8. Document the disaster recovery plan. The last official activity of the cross-functional team is to document the disaster recovery plan for use by the recovery team, which will then have responsibility for maintaining its accuracy, accessibility, and distribution. Documentation of the plan must also include up-to-date configuration diagrams of the hardware, software, and network components involved in the recovery.

9. Plan and execute regularly scheduled tests of the plan. Disaster recovery plans should be tested a minimum of once a year. Progressive companies test three or four times annually. Maintain a checklist during the test to record the disposition and duration of every task, and compare it to the list of planned tasks. Consider developing a test plan that spans up to three years—every six months the tests can become progressively more involved, starting with program and data restores and followed by processing loads and print tests, then initial network connectivity tests, and eventually full network and desktop load and functionality tests.

10. Conduct a lessons-learned postmortem after each test. The intent of the lessons-learned postmortem is to review exactly how the test was executed as well as to identify what went well, what needs to be improved, and what enhancements or efficiencies could be added to improve future tests.

Nightmare incidents

During many years of managing and consulting on IT infrastructures, I've encountered a number of nightmarish disaster recovery incidents. Some are humorous, some are "head-scratching," and some are just plain bizarre. In all cases, they totally undermined what would have been a successful recovery from either a real or simulated disaster. Fortunately, no single client or employer with whom I was associated ever experienced more than any two of these, but in their eyes, even one was unacceptable. These incidents, listed below, illustrate how critical planning, preparation, and performance are to a good disaster recovery:

- Backup tapes have no data on them.
- Restore process has never been tested.
- Restore tapes are mislabeled.
- Restore tapes can't be found.
- Offsite tape supplier hasn't been paid and can't retrieve tapes.
- Graveyard-shift operator doesn't know how to contact recovery service.
- Recovery service to a classified defense program is not cleared.
- Recovery service to a classified defense program is cleared, but individual personnel aren't cleared.
- Operator can't carry tape canister onto the airplane.
- Tape canisters are mislabeled.

The first four incidents all involve the handling of the backup tapes required to restore copies of data rendered inaccessible or damaged by a disaster. Verifying that the backup and, more importantly, the restore process are completing successfully should be one of the first requirements of any disaster recovery program. While most shops verify the backup portion of the process, more than a handful of shops don't test to verify that the restore process also works. Labels and locations can also cause problems when tapes are marked or stored improperly.

Although a rare case, I do know of a client who was unable to retrieve a tape because the offsite tape storage supplier hadn't been paid in months. Fortunately, it was not during a critical recovery.

Communication to, documentation of, and training of all shifts on the proper recovery procedures are critical. Third-shift graveyard operators often receive the least of these due to their off hours and higher-than-normal turnover. These operators need to know whom to call and how to contact offsite recovery services.

Classified environments can present their own brand of recovery nightmares. One of our classified clients had applied for a security clearance for its offsite tape storage supplier and had begun using the service prior to the clearance being granted. When the client's military customer found out, the tapes were confiscated. In a related issue, a separate defense contractor cleared its offsite vendor to a secured program but failed to clear the one individual who worked nights when a tape was requested for retrieval. The unclassified worker couldn't retrieve the classified tape that night, delaying the restoration of the data for at least a day.

The last two incidents involve tape canisters used during a full dry-run test of restoring and running critical applications at a remote hot site 3,000 miles away. The airline in question had just changed its carry-on baggage policy, which meant the recovery team couldn't keep the tape canisters with them. Making matters worse was the fact that the canisters were mislabeled, which cost over six hours of restore time. There was much to talk about during the marathon postmortem session that followed this incident.

Rick Schiesser is a part of The Harris Kern Enterprise Computing Institute, a consortium of leading industry experts responsible for the design and implementation of world-class IT organizations. For more information on the Harris Kern Enterprise Computing Institute, visit www.harriskern.com.

Responsibility

General responsibilities pertaining to this policy are set forth in this section, as well as any pertinent specific responsibilities.

Scope

[For internal employees]: This policy applies to all employees, contractors, consultants, temporaries, and other users at [insert company name], including those users affiliated with third parties whose work necessitates the use of instant messaging software while performing work at [insert company name] or using any company-owned or affiliated data communication systems.

[For external employees]: This policy applies to all employees, contractors, consultants, temporaries, and other users at [insert company name], including those users affiliated with third parties that access [insert company name]'s computer networks. The policy also applies to all computer and data communication systems owned by and/or administered by [insert company name]'s authorized contractors or consultants.

Programs

Although subject to changes, [insert company name] has adopted [identify IM application here; i.e., *only one external commercial instant messaging service: America Online Instant Messenger (AIM*)].

Company-installed computers

All company PCs that will need IM software will have [IM application name] installed by the IT department and will generally follow this user format:

Screen name: [insert company name](first name)

Password: [insert company name](default) (The user can change the password.)

Although the IT department does not fully support the IM software, IT will provide basic training on the software and help to users.

Personally owned installed computers

If the user has an existing [insert IM application name] screen name that he or she wishes to use, the user must e-mail the screen name to the IT department if you would like to communicate with [insert company name] employees via [insert company name]'s data communication systems.

Responsibilities

IT manager

The overall management of the IM policy, IM usage and monitoring, and IM equipment maintenance are the responsibility of the IT manager. The IT manager will coordinate all company-authorized IM installations. Individuals must contact the IT manager if they wish to request any changes.

Users that install IM on their own equipment may not necessarily be provided with technical support.

Department manager

Department managers are responsible for monitoring individual employees' IM use and deeming whether the usage is appropriate. Department managers and company officers have the right to review, question, and verify information sent using [insert company's name] data communication systems. Department managers will provide within their budget for any equipment or services that they deem necessary for company business.

Individual users

Employees must obtain departmental approval prior to using or installing any IM software or hardware, and they must use only the company's internal or external IM client and services to communicate with fellow employees or business associates.

If asked to do so, employees are required to surrender all IM-related material provided for them to the company in a timely matter and discontinue the use of the [insert company name]-based username.

Use only the company's internal or external IM client and services to communicate with fellow employees or business associates.

IM carrier/service provider services

IM carriers and service providers have begun to provide various additional services for IM users. Unless a policy is approved and distributed, [insert company name] does not currently support or pay for the use of chargeable services like business location information, reservations, movie times and locations, etc. The IM user is fully responsible for any additional charges related to carrier services that he or she may incur.

IM access via a cell phone

Unless a policy is approved and distributed, [insert company name] does not currently support or pay for the use of IM services or Web time via a cell phone.

Additional IM features

Unless a policy is approved and distributed, [insert company name] does not currently support or pay for the use of downloadable ringers, tones, playing MP3 music files, and other nonessential extras via an IM session.

Personal IM messages

IM messages relayed via company data systems for personal reasons, outside of emergencies or notifying significant others of working extremely late, are to be kept at a minimum and will never interfere with normal data communication services. Employees will also be held responsible for “charges” that occur due to unauthorized use of the IM software.

IM etiquette

- Do NOT discuss confidential or sensitive company business or information through any public IM services.
- Do not open or accept IM attachments transmitted through a public IM service. ALL attachments/files will be sent via the company e-mail system.
- Be aware that all IM conversations on the company's network system should not be considered private.

IM security

- If you think that your IM username or session has been compromised, shut down your session immediately and call the IT manager as soon as possible. If the compromise occurs after hours, shut down your session as well as your Internet connection and call the IT manager as soon as possible.

- Employees, contractors, consultants, temporaries, and other users at [insert company name], including those users affiliated with third parties that use company data systems or IM equipment and are representing the company, and are thus responsible for ensuring that the equipment or IM service is used in an effective, ethical, and lawful manner.
- At no time is the username/ID to be disabled. Users are responsible for the content of all communication sent and received over the IM service provider's system. Don't say anything in your IM conversations or in the e-mail messages that you wouldn't want to see on the front page of the newspaper or be required to explain in a court of law.
- All messages created, sent, or retrieved over the company's IM system are the property of the company and may be regarded as public information. [Insert company name] reserves the right to access the contents of any messages sent over its systems if the company believes, in its sole judgment, that it has a business need to do so.
- Credit card numbers, telephone calling-card numbers, login passwords, and other information that can be used to gain access to the goods or services of [insert company name] must not be sent in readable form over the Internet or IM sessions to anyone at any time.

Authorized usage

[Insert company name]'s communications systems generally must be used only for business activities. Incidental personal use is permissible if required because of an immediate or emergency situation. IM users are forbidden from using [insert company name]'s electronic communications systems (including cell phones, pagers, and e-mail) for charitable endeavors, private business activities, or amusement/entertainment purposes unless expressly approved by the [insert company name] president or his or her representative.

Employees are reminded that the use of company resources, including electronic communications, should never create either the appearance or the reality of inappropriate use. Activities such as harassment, threats, etc., made on an IM chat session or other electronic communication devices provided by the company are not condoned and will result in immediate disciplinary action.

Acknowledgment of company IM policy

This form is used to acknowledge receipt of, and compliance with, the [insert company name] IM policy.

Procedure

Complete the following steps:

1. Read the IM policy.
2. Sign and date in the spaces provided below.
3. Return this page to the IT manager.

Your signature indicates that you have read [insert company name]'s IM policy. Signing this document does not mean that you agree with each and every provision of the policy. However, it does mean that you will abide by the regulations set forth in the above policy. By signing below, I agree to the following terms:

1. I have received and read a copy of the [insert company name] IM policy, and I understand the same.
2. I agree that, if I leave [insert company name] for any reason, I shall immediately return to the company any equipment that I may have received from the company that is either in my possession or otherwise directly or indirectly under my control and will discontinue the use of any communication device or IM user ID that was provided.
3. I also agree that, if I leave [insert company name] for any reason, that I bear all financial responsibility for any termination fees or continued plan usage. I agree that [insert company name] is not financially responsible for any termination fees or continued plan usage.
4. I agree that I will adhere to the regulations set forth in the IM policy.

Employee signature:

Employee name:

Date:

Network documentation outline

Items necessary for good network documentation

1. Identification of servers, workstations, printers, routers, switches, etc.
    a. IP addresses
    b. NetBIOS/Host names
    c. MAC addresses
2. Description of each device on the network, including make, model, serial number, and printouts from system inventory software (such as Belarc Advisor)
3. Network topology diagrams, including placement of servers, routers, switches, firewalls, IDS, etc.
    a. Physical and logical diagrams
    b. Layer 3 networking diagrams, including backbone and WAN links
4. Internet provider information
    a. Description of link(s)
    b. Contacts and support numbers
    c. Terms of service
5. List of supported network operating systems (Win2K Server, NT4, NetWare 5, Linux, etc.)
6. List of supported client operating systems (Win2K Pro, Win98, MacOS, Linux, etc.)
7. List of supported network protocols (TCP/IP, IPX/SPX, AppleTalk, NetBEUI, etc.)
8. DHCP server settings, including scopes and options
9. Network security settings
    a. Firewall configuration (including TCP and UDP ports open)
    b. Router access lists
10. Troubleshooting history/administrator's activity log
    a. Common problems and resolutions
    b. Installation history
11. Network baseline information
    a. Traffic flow and network utilization
    b. Bandwidth utilization
    c. Percent of collisions
    d. Average server and workstation CPU utilization
    e. Average server and workstation memory utilization
12. Fault tolerance mechanisms in place
    a. Disk redundancy (e.g., RAID arrays)
    b. Tape backup plan, including rotation and off-site storage
    c. Clustering and failover systems
13. Physical location documentation
    a. Building map
    b. Room numbers
    c. Availability of access keys
    d. Unusual configuration information
14. Policies and procedures
    a. Naming conventions
        i. Workstations and servers (NetBIOS and host names)
        ii. Network equipment (e.g., routers and switches)
        iii. Active Directory
        iv. DNS
    b. Points of contacts (IT director, administrators, help desk, etc.)
    c. Disaster recovery plan
        i. Vendor phone numbers for support

ii. Remote access plan for administrators
iii. Higher-up administrator or consultant on call
iv. Virus prevention/recovery plan

d. Copies of maintenance plans, warranty agreements, and tech support contacts
e. Software licensing information
f. User rights policies, including Internet and e-mail usage

Password policy

Acme, Inc.

Overview

Purpose

This policy outlines the handling, responsibilities, and scope of passwords for the Information Technology (IT) resources of Acme, Inc. This policy acts as an extension of the IT security policy for Acme, Inc.

Authority

This policy has full support from the Acme, Inc., executive steering committee and human resources department. The IT manager administers the policy, which is currently effective for all Acme, Inc., employees and computer systems.

Password policy

Mission

The IT objective of Acme, Inc., is to enable Acme employees to perform their tasks with technology that is in good operating condition while appropriately addressing the business needs and keeping information secure within our IT resources.

The Acme, Inc., password dilemma

Passwords are the entry point to our IT resources. Protecting access to our resources is pivotal in ensuring that our systems remain secure. While we have not been exploited, nor do we expect to be, we must be diligent in guarding access to our resources and protecting them from threats both inside and outside our organization.

Password handling

Passwords for *all* systems are subject to the following rules:

- No passwords are to be spoken, written, e-mailed, hinted at, shared, or in any way known to anyone other than the user involved. This includes supervisors and personal assistants.
- No passwords are to be shared in order to "cover" for someone out of the office. Contact IT, and it will gladly create a temporary account if there are resources you need to access.
- Passwords are not to be your name, address, date of birth, username, nickname, or any term that could easily be guessed by someone who is familiar with you.
- Passwords are not be displayed or concealed on your workspace.

Systems involved

The Acme, Inc., password policy will address the passwords for the following IT systems with their rules:

- **Network and client operating system**: Windows 2000 username and password (Users will automatically be prompted at a login to change the password every 45 days.)
- **Outlook/Exchange groupware**: Windows 2000 username and password (Users will automatically be prompted at a login to change the password every 45 days.)

- **Computer BIOS password**: Hardware-level access to your computer (This password will not automatically change.)
- **VPN password**: The Acme, Inc., telecommuting system (Users will be prompted to change this password once a year.)
- **ERP system**: SAP credentials to the production system (Users will be prompted to change this password once a year.)
- **WWW accounts**: Credentials to external Web resources (These passwords are rarely changed unless initiated by the user. IT has disabled the option for these credentials to be saved [IE password caching] on all Acme, Inc., computers.)

Password composition

The following systems have systematically enforced password requirements as stated:

- **Network and client operating system (and Outlook)**: Passwords must meet the following criteria:
  - Password may not contain all or part of the user's account name.
  - Password is at least six characters long.
  - Password contains characters from three of the following four categories:
    - English uppercase characters (A…Z)
    - English lowercase characters (a…z)
    - Base 10 digits (0…9)
    - Nonalphanumeric (exclamation point [!], dollar sign [$], pound sign [#], percent sign [%], etc.)

Support

All Acme, Inc., users are to contact the IT staff for support of the password policy. IT welcomes your questions and suggestions and strives to keep our resources secure.

Administrative passwords

Administrative passwords are subject to stringent composition, frequent change, and limited access. This includes passwords for routers, switches, WAN links, firewalls, servers, Internet connections, administrative-level network operating system accounts, and any other IT resource.

Passwords for administrative resources must meet the following criteria:

- Password is at least 10 characters long.
- Password contains mixed case.
- Password contains at least three nonalphnumeric characters.
- Password contains at least two numbers.

Responsibilities

IT has the responsibility to enforce this policy. This can be done through systematic means and interaction with users.

Acme, Inc., users are responsible for complying with this policy.

Continuance

This policy is a living document and may be modified at any time by the IT manager, the executive steering committee, or the human resources department.

Summary

This policy is designed to secure Acme, Inc., resources. This enables Acme, Inc., to achieve its business objectives. Full cooperation with this policy is appreciated so that all goals can be met in accordance with the business objectives.

(SAMPLE)
GENERAL COMPUTING POLICY

THIS AGREEMENT (the “Agreement”) is hereby made and entered into by and between [COMPANY] (herein, “Company”) and ____ (herein, “You” or “Employee”) and entered into on this date: _______________________.

You hereby warrant that you agree and understand that as an Employee, you are responsible for securing the company's network and computing systems against unauthorized access and/or abuse. Any attempt to violate any provision of this policy will result in disciplinary action, up to and including immediate termination.

You hereby warrant that you agree and understand that as an Employee you are responsible for obeying all local, state, federal and international laws regarding the use of our computers. Any attempt to break those laws through the use of the Company's computers or network may result in charges and fines being levied against you. In such an event, You hereby agree and understand that the Company will fully cooperate with authorities to provide any information necessary.

You further hereby warrant that you agree with and understand the following:

SECTION 1: GENERAL COMPUTING AND OFFICE POLICY

When you receive a user ID to be used to access the network and computer systems on that network, including both our internal network and any external network such as the Internet and commercial online services, you hereby agree and understand that you are solely responsible for all actions taken while using that user ID. And that:

1. Applying for a user ID under false pretenses is a punishable disciplinary offense.
2. Sharing your user ID with any other person is prohibited. In the result that you do share your user ID with another Person, you will be solely responsible for the actions that other person appropriated.
3. Deletion, examination, copying, or modification of files and/or data belonging to other users without their prior consent is prohibited.
4. Use of facilities and/or services for other commercial purposes if prohibited.
5. Use of facilities and/or services for entertainment purposes is prohibited.
6. Use of facilities and/or services for immoral, illegal or unethical purposes if prohibited.
7. Any unauthorized, deliberate action, which damages or disrupts a computing system, alters it normal performance, or causes it to malfunction, is a violation regardless of system location of time duration.
8. Removal of any company property is prohibited.
9. Use of company fax machine, postage machine and copier is for business purposes only.

SECTION 2: GENERAL E-MAIL & VOICE MAIL POLICY

You hereby agree and understand that both the Company’s e-mail, Internet access, and voice mail systems (which are provided for your use) are for business use only. As such, you hereby agree and understand that the company may monitor both e-mail, Internet access and voice mail systems at will, including the full content of any messages therein, without further disclosure to you. You hereby warrant that you understand that whenever you send electronic mail, your name and user ID are included in each mail message. You are, therefore, responsible for all electronic mail originating from your user ID. Further:

1. Forgery (or attempted forgery) of electronic mail messages is prohibited.
2. Attempts to read, delete, copy, or modify the electronic mail of other users are prohibited.
3. Attempts at sending harassing, obscene and/or other threatening email to another user if prohibited.
4. Attempts at sending unsolicited junk mail, “for-profit” messages or chain letters is prohibited.

SECTION 3: NETWORK SECURITY POLICY

As a user of the network, you may be allowed to access other networks (and/or the computer systems attached to those networks). Therefore:

1. Use of systems and/or networks in attempts to gain unauthorized access to remote systems is prohibited.
2. Use of systems and/or networks to connect to other systems, in evasion of the physical limitations of the remote system/local, is prohibited.
3. Decryption of system or user passwords is prohibited.
4. The copying of system files is prohibited.
5. The copying of copyrighted materials, such as third-party software, without the express written permission of the owner or the proper license, is prohibited.
6. Intentional attempts to “crash” Network systems or programs are punishable disciplinary offenses.
7. The attempts to secure a higher level of privilege on Network systems are punishable disciplinary offenses.
8. The willful introduction of computer “viruses" or other disruptive/destruction programs into the organization network or into external networks is prohibited.

This is a legally binding-Contractual Agreement. Some or all-of the provisions contained herein may survive your employment with The Company. Your signature below indicates that you thoroughly understand and accept these policies as a material condition of your employment and that any violation of any of these provisions may result in severe disciplinary action by the company against you up to and including immediate termination.

AGREED to the date first written above, the parties signed in agreement.

For and behalf of [COMPANY]:

____

Date:

____

Employee:

Name (please print):

____

Date:

____

Signature:

____

Software installation policy

Acme, Inc., information technology software installation policy

Overview

Purpose

The purpose of this policy is to address all issues relevant to software installation and deployment on Acme, Inc., computer systems.

Authority

This policy has full support from the Acme, Inc., executive steering committee and human resources.

The information technology (IT) manager administers this policy. This policy is currently effective for all Acme, Inc., employees and computer systems.

Continuance

This policy is a living document and may be modified at any time by the IT manager, human resources, or the executive steering committee.

Software installation policy

Mission

Acme, Inc.'s IT objective is to enable Acme employees to perform their tasks with technology that is in good operating condition while appropriately addressing the business needs.

Dilemma

Historically, we have not consistently addressed how software is to be deployed to Acme, Inc.'s computer systems. This lack of a standard policy has adversely affected the IT mission at times. This policy will set protocol as to how software is to be delivered to better enable IT to achieve its objective of delivering stable, well-performing technology solutions.

Installation and support of Acme, Inc., software

The Acme, Inc., IT department is exclusively responsible for installing and supporting all software on company computers. This responsibility set includes:

- Office desktop computers.
- Company laptop computers.
- Computer lab public desktop computers.
- Telecommuter home computers (provided by the company).

The Acme, Inc., IT department relies on installation and support to provide software and hardware in good operating condition to Acme, Inc., employees so that they can best accomplish their tasks.

Current software

Acme, Inc., IT, in coordination with all other departments, has decided upon the following software standards:

Desktop operating system

- Microsoft Windows NT 4.0 with critical updates, shutdown supplement

Productivity tools package

- Microsoft Office 97 with Service Release 2a
    - Word
    - Excel
    - PowerPoint
    - Access (Professional Edition users only)
    - Outlook 98

Manufacturing software

- SAP R/3 workstation
- Oracle client software

Financial software

- Commander FDC workstation

Tax accounting software

- AACTS workstation
- CCH CD-ROM client software

Human resources software

- ABRA client
- BNA HR Library client software

Internet software

- Netscape Navigator 4.05 with 128-bit encryption
- Real Audio Player 8 Plus
- Microsoft FrontPage Express 2.0

Accessories

- WinZip 8.0
- Adobe Acrobat Reader 3.02
- McAfee VirusScan 4.5

The current software can exist in any one of the following scenarios:

- An IT-created "image" or OEM installation on the hardware
- An Acme, Inc., IT department installation procedure that provides for the following:
    - Installation options
    - Upgrade considerations (if applicable)
    - Data conversion (if applicable)
- A shortcut to a network application (not truly an installation)
- An automated installation through an IT-developed solution that may be used in a rapid-deployment scenario or silent-install situation
- A terminal application, Citrix application, or other thin-client type of application accessible via the Acme, Inc., intranet page

Software **cannot** be present on Acme, Inc., computers in the following scenarios:

- An installation not by a procedure
- A piece of software purchased for one's home computer
- A downloaded title from the Internet
- A pirated copy of any title
- A different title from the current software list of this policy
- Any means not covered by the ways that software can exist on Acme, Inc., computers

Software licensing

Most of the software titles on Acme, Inc.'s current software list are not freeware; therefore, the cost of software is a consideration for most titles and their deployment.

It is the goal of the IT department to keep licensing accurate and up to date. To address this, the IT department is responsible for purchasing software licenses for the following software categories:

- Desktop operating system software
- Productivity tools package
- Internet software
- Accessories

The other software categories (workgroup-specific titles) are the purchasing responsibility of the workgroup in which they serve. However, the application(s) are still installed and supported by the IT department.

To control costs, licensing costs are a factor in the decision-making processes that go into client software planning and request approval.

Software requests

If a user is to request software for their computer, the proper method will be to fill out the Acme, Inc., support request on the intranet at: http://intranet.acme.net/support_request.asp. This form is also available by following the IT links on the Acme, Inc., intranet home page, which is the start page of all Acme, Inc., Web browsers.

The intranet site is also a means to suggest additions to the current software set for Acme, Inc., and it contains a form for requesting new software for your machine. This form submits a request into the IT support database. A response is guaranteed within one business day via e-mail. If the Urgent option is selected or an in-person appearance occurs, a solution may be delivered at the first possible time. All in-person or “walk-in” requests are logged by a manual entry into the support request system to track licensing needs and costs.

Summary

Acme, Inc., software installation policy

This policy is designed to let Acme, Inc., employees achieve their business objectives. Any aberrations from this strategy will require the IT department to redeploy software and/or hardware solutions. Full cooperation with this policy is appreciated so that all goals can be met in accordance with the business objectives.

Get the word out: Information systems security is part of everyone's responsibility

If a picture is worth a thousand words, you've just downloaded over 5,000 words worth of training materials.

To protect information managed and stored on corporate computers—and the computers themselves—every employee is responsible for doing his or her share. If you're like most IT shops, you've published policies and sent out global e-mail messages about best practices to end users of your systems. In this document, you'll find another trick you can add to your awareness campaign: posters you can display on the bulletin boards in your company cafeteria, include in e-mail messages to all users from the IT department, or add to your agenda for new-employee orientation.

Can a handful of posters help reduce help desk calls and increase awareness about security issues? The answer is, yes. If just one end user reads the poster and refrains from watering a plant on top of a computer monitor or another end user stops writing his or her password on a sticky-note hidden under the monitor, consider the posters a success.

Feel free to customize these documents for your shop. The posters I've included here are:

- Log Off Before You Run Off
- Please Don't Water the Equipment
- IT Corporate Software Policy
- Protect Your Password
- Help Desk Contact Information

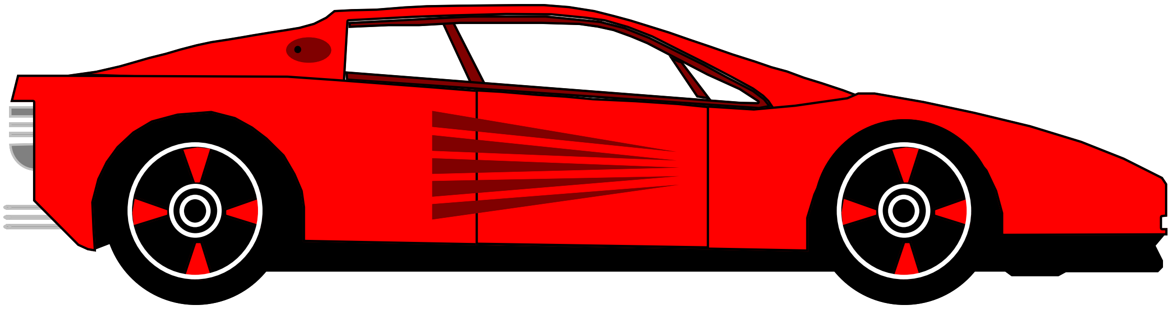
Good luck with your IS awareness training. To let us know what you think about these posters, please drop us a note.

Jeff Davis
Help Desk Advisor Columnist, Support Republic

LOG OFF

BEFORE YOU RUN OFF

If you leave your automobile running and unattended,



someone may steal it.

If you leave your workstation without locking it or logging off,

someone may steal your ID

and send e-mail from you

or surf the Web to an inappropriate Web site.

LOG OFF OR LOCK YOUR WORKSTATION

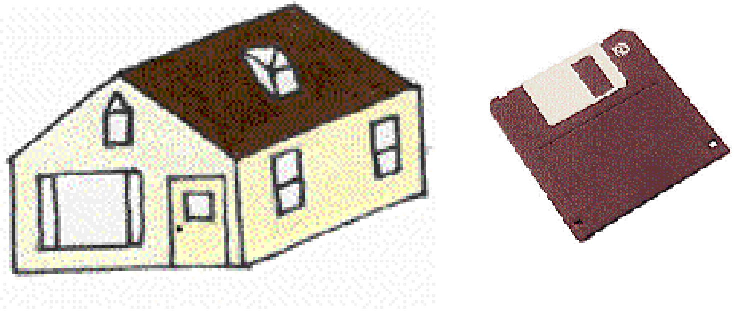
BEFORE YOU RUN OFF!

Please don't water the equipment.

IT Corporate Software Policy:

Only authorized software may be installed on company computers.

No software from home



and no software downloaded from the Internet

PROTECT YOUR PASSWORD

User name: yourna

Password:

NEVER:

☒ Share your password with someone else.

☒ Write down password where others can see it.

☒ Discuss your password outside work.

The Corporate Assets You Save May Be Your Own.

HELP DESK AWARENESS

Need tech support?

Help Desk Regular Business Hours Extension____________

Emergency Pager Dial___________________

Corporate Intranet http://www.____________

If you see something or someone suspicious, notify the security department at extension ________.

Welcome letter

www.techrepublic.com

Welcome from the IT Department! We are providing this information to help you get started using your computer. If you have any questions, please contact the Help Desk at ext. XXX.

Your computer was set up by _____________________ at extension ____________.

Logon and password	To log on to the system, press [Ctrl][Alt][Delete]. For the User ID, type your first initial and your last name without spaces. Be sure to use all lowercase letters. The first time you log on to the system, enter *password* for the password. The system will then ask you to change your password. Your password must be at least eight characters and must include at least one number. Your new password is case-sensitive.
Phone stuff	Your telephone extension is ______. To check voice mail, press the Messages button. The first time you check messages, enter 1234 as the password. The system will then ask you to change your password. Your voice-mail password must be at least four digits long and must be a number from zero through nine. The password cannot contain a pound sign (#) or an asterisk (*).
Printer stuff	The default printer that has been installed for your computer is named PTR___ and is located in Room ___. If you need help installing additional printers, please call the Help Desk at ext. XXX.
Fax stuff	Fax messages for you should be sent to XXX-____. The fax machine is located in Room ___.
Software Installed on your computer	___Standard desktop applications (e-mail, word processing, spreadsheet, Web browser) ___Standard laptop applications (e-mail, word processing, spreadsheet, Web browser, dial-up access) ___Database/development tools ___Graphics ___Computer-aided design

Frequently Asked Questions

What if I can't log on?	Call the Help Desk at ext. XXX.
What if I can't get into the e-mail system?	Call the Help Desk at ext. XXX.

What if I forget my new password and get locked out of the system?	Call Client Systems at ext. XXX. They will reset your password, and you will have to create a new one the next time you log on.
Should I turn off my computer before I leave work?	No. Always leave your computer on. Before you leave work, log off the system but leave the computer turned on.
Should I ever lock my workstation?	Yes. You should lock your workstation any time you leave your desk for more than five minutes.
What if I can't print?	Install network printer ____ or call the Help Desk at ext. XXX.
What if I need access to a color printer?	Install network printer ____ or e-mail the Help Desk.
What if I need additional software installed on my computer?	Your manager will need to approve your request and forward it to call Client Systems.
What if I need to move my computer to another location?	Before you do, please call Hardware Support at ext. XXX.
Can I contact the Help Desk on the Web or by e-mail?	The Online Help Desk Web site is:_____________________ The Help Desk e-mail address is:_____________________
What if I need computer help after regular business hours?	Call the Help Desk at (XXX) XXX-XXXX. In emergencies, page the on-call support person at (XXX) XXX-XXXX.

Wireless communications policy

The [*insert company name*] wireless communications policy is to provide services and limited support for cellular phones, paging, and other wireless communications devices to employees who have a recognized business requirement and have the approval of their managers for the expenses involved.

Specific details are covered in the sections that follow. All direct company expenses associated with wireless services will be charged to user department budgets. Because of the indirect administrative costs involved in managing these services, company-sponsored wireless services are restricted based upon the type of service and the individual user's responsibilities.

[*Insert company name*] Telecom provides company-sponsored cellular service on corporate accounts for higher-level management employees (associate vice president and above). For employees below the AVP level, [*insert company name*] will allow reimbursement of equipment and monthly cellular expenses based upon corporate guidelines at the discretion of the individual employee's manager. Such reimbursement must be requested through the company's expense reporting process and will require normal managerial approvals.

Vendors

Employees on company-sponsored cellular plans will be limited to the vendors, equipment, and service plans available in our established accounts (currently XXX vendors and XXX types of phones). Employees eligible for company-sponsored cellular plans that wish to use a different vendor and/or who wish to use equipment not offered under existing standards may choose to make their own selections and request reimbursement through the expense reporting process. Such reimbursement will be at the discretion of the employee's manager.

Due to administrative burdens, the company is pursuing a user self-help approach to supporting wireless services wherever feasible. Toward that goal, cellular telephone users will generally need to address issues directly with their cellular service providers. However, [*insert company name*] does offer full support of company-owned [*insert device name*] pagers and [*insert device name*] pagers leased through [*insert vendor(s) name(s)*].

Device use

It is the responsibility of each employee to use reasonable care in handling and protecting wireless devices provided by or paid for by the company. Corporate insurance policies cannot cover this type of loss. Should such equipment be lost, stolen, or damaged beyond repair, replacement costs must be borne by either the responsible employee or by the employee's department at the discretion of the employee's manager and depending upon the circumstances of the loss.

Company-sponsored cellular phones

The company will order and add a cellular phone to the corporate account for an employee at or above the position of associate vice president who requires the use of a cellular phone to perform his or her job responsibilities. Cellular phones covered under this policy are limited to those that are currently supported by the company.

[*Insert company name*] supports a limited number of phone types and offers service through [*insert number*] providers: [*List below service vendors and phone brands supported, also indicating company preference on international service.*]

Wireless device request process

An employee’s manager must submit written (e-mail) authorization to [*insert company name*]’s telecom division requesting a cellular phone for the employee. If additional accessories (headset, spare battery, spare charger) are required for use with the phone, this must be requested in writing at the time the order is placed. Due to the administrative burden to the company, accessory requests made after the cellular order has been placed will be the responsibility of the employee to complete. The decision whether to purchase other auxiliary equipment after the initial cellular order is at the manager's discretion. If a manager approves reimbursement of such an expense, this must be done through the expense report process.

Should an employee desire a type of cellular telephone or a cellular service provider that is not supported, the employee is responsible for the procurement of and payment for that phone as detailed in the "Employee-owned cellular phones" section of this policy.

Monthly fees for service will be paid for by the company and billed to the department in which the employee works. Reimbursement of excessive cellular charges may be requested and approved at the manager's discretion.

The cellular service provider will handle day-to-day maintenance and support. [*Insert vendor name*] can be reached at [*insert vendor phone number*].

Reporting phone loss, damage incident

Should an employee's cellular phone be lost, stolen, or damaged beyond repair, the company will pay for a replacement only upon approval of the expense by the employee's manager. Costs for replacements will be billed to the employee's department. Employees will not be permitted to upgrade equipment as a result of losing or damaging it. Because company insurance policies are unable to cover the replacement cost of cellular phones, employees must follow this procedure when cellular phones are lost or stolen.

[*If applicable, include information on vendor's insurance policy and deductible requirement. List vendors, contact phone numbers, and specific steps (see example below) required to report insurance claim.*]

To take advantage of [*vendor*] insurance, the employee must take the following steps:

- Notify help desk of the loss.
- Notify [*insert vendor name*] at [*insert contact phone number*] so they can flag the phone as stolen. Be sure to ask for your phone's IMEI number and record the ticket number that [*insert vendor name*] will provide.
- Employees must use their personal credit card to pay for the cost of a replacement phone and order equipment identical to what was lost.
- If warranted, request reimbursement of the expense through the expense reporting process with manager's approval.

In the event of a staff termination/resignation

Company-owned cellular phones must be turned in to [*insert company name*]'s human resources department when the employee leaves the company. Any accessories provided with the phone, or paid for by [*insert company name*] through the expense process, must be turned in with the phone at the time of exit, as they are the property of the company.

Employee-owned cellular phones

If an employee occupies a position below associate vice president, or if an employee prefers a nonsupported phone to those inventoried, [*insert company name*] provides the following options:

An employee may be reimbursed for the purchase of cellular phone equipment with monthly service from the provider of choice if the phone's use is a requirement of the employee's position. The employee will establish a contract with the provider and be financially responsible for the timely payment of the monthly expense. Reimbursement of these expenses may be requested through the expense report process and is at the discretion of the employee's manager. The employee will own the equipment and service plan should he or she leave the company.

Although the amount to be reimbursed will be at the manager's discretion, the typical cost for a new phone with activation is approximately $50. Monthly service cost will vary based on usage but should run between $40 and $185.

It is recommended that manager and employee discuss equipment and calling-plan costs before the employee commits to a service contract. A calling plan should be selected with a sufficient number of base minutes to accommodate the employee's monthly usage. Some plans may also offer no roaming or long-distance charges. For users who travel frequently or make a lot of long-distance calls, these plans are recommended, since lesser plans will simply charge greater amounts for these services when they are used. As service providers are usually willing to renegotiate service agreements, an employee who regularly goes over or falls short of his/her plan usage should discuss this with his/her manager and agree on a calling-plan modification that will help bring the cost in line.

Any purchase of additional equipment, such as batteries, headsets, speakerphone modules, car lighter adapters, carrying cases, etc., will be the choice and responsibility of the user. Approving managers should carefully evaluate accessory purchases and consider what is appropriate to reimburse. A second battery is rarely needed, while a headset may improve safety for employees who use their phones while driving. Some approximate accessory costs are listed below:

Headset:	$20
Belt clip:	$6-$12
Leather case:	$10-$15
Spare battery:	$60-$100
Dual-port charging stand:	$70
Car lighter adapter:	$20-$40

The company will reimburse the employee for the cost of cellular business calls or service plan up to a maximum of $185 per month, including business-related roaming charges and monthly service fees related to business use. Exceptions to this limit must be fully justified by the particular business situation involved. Should there be a significant blending of business and personal usage, manager and employee may choose to expense costs on a prorated basis by establishing a fixed percentage of the monthly service cost to be reimbursed.

To be reimbursed for business-related cell phone calls, the employee must fill out an expense report and submit the approved expense report to Accounts Payable on a monthly basis.

Any cost associated with damage, loss, or theft is the sole responsibility of the employee. At the manager's discretion, [*insert company name*] may reimburse the modest cost of equipment insurance from the cellular service provider.

Should the monthly fees for an employee's use of his or her phone extend over the usage plan, the overage cost is the sole responsibility of the employee. It is expected that the employee and manager will monitor monthly costs and anticipate changes in behavior that may merit changes to the plan. Events that need to be considered in contemplating changes to rate plans include the following:

- New responsibilities that require more out-of-area travel on company business will increase roaming as well as long-distance charges.
- An increase in monthly minutes used may go over the base number of minutes included in the plan, thereby increasing the cost.
- Traveling to Canada will incur more costly roaming fees that cannot be avoided by changing the calling plan.
- Making international calls from a cell phone will incur long-distance charges that cannot be avoided by modifying the plan.

International calling requirements

Users who activate international dialing capability on cellular phones may incur excessive costs. The use of cellular phones for international dialing is strongly discouraged except where unavoidable. Time differences may dictate cellular use as a necessity, but a calling card should be used whenever possible to decrease this expense. Calling card savings can be as much as 90 percent over international cellular use, both at home and abroad.

Traditional paging services

- Should an employee’s job require him or her to carry a pager, the company will issue a pager according to the following guidelines:
- The employee’s manager must submit written (e-mail) authorization to [*insert vendor name*] Telecom requesting a pager for the employee.
- Paging service will be provided from one of [*insert company name*]'s [*insert number*] approved paging vendors: [*List vendors and service levels.*]
- [*Insert vendor name*] Telecom will issue a pager to the employee and arrange for the cost of the device to be charged to the employee’s department on a monthly basis.
- [*Insert vendor name*] Telecom will arrange a paging alias to be associated with the pager so that e-mails sent to page-username@XXX.com will be forwarded to that pager.
- When the pager is issued, the employee will be given customer service information for the relevant paging company. Should the employee experience any difficulty with the pager, it is the employee’s responsibility to contact the paging company to troubleshoot the difficulty. It is always recommended to confirm that your alias is set up properly before contacting the vendor.
- If the pager is lost, stolen, or damaged, the employee must notify [*insert vendor name*] Telecom at once. The employee’s department must pay for the cost of repair or replacement. Reimbursement for the pager may be requested from the employee at the manager’s discretion.
- If the employee’s need for a pager should pass, or if other communication methods are adopted to replace the pager, the pager must be turned in to [*insert vendor name*] Telecom.
- The pager must be turned in to [*insert company name*]'s HR department or the telecommunications manager upon moving to another department or leaving the company.

BlackBerry Pagers [*Or insert other specific pager devices and list appropriate information.*]

A BlackBerry pager is a unique device that allows the user to access his/her Outlook Exchange account from a wireless pager. Manufactured by Research In Motion (RIM), the BlackBerry is not equivalent to traditional paging, as coverage is less complete and may not exist in some areas. Present corporate policy is designed to control the dissemination of BlackBerry wireless units in order to keep vendor and internal support costs to a manageable level. As these units are not particularly robust, the effort and cost of providing them on a large-scale basis is prohibitive. However, because of the extremely time-sensitive communications requirements of certain management functions and the potential for impacting the operations of the company, the use of these units is supported for director-level management and above who have mission-critical needs for immediate notification and response to e-mailed messages.

Only company-sponsored and provided devices are supported. Direct costs for the equipment and monthly service are included on the corporate account and charged back to the user’s department.

The cost for a BlackBerry 950 pager is $XXX for the device and a $XXX flat rate monthly for service. The contract term is XXX years.

The employee’s manager must submit a request via e-mail to [*insert company e-mail address*] stating that he or she is aware of the expense and requires the employee to carry the BlackBerry in order to perform job responsibilities.

Equipment is ordered as needed, so please request BlackBerrys XX weeks in advance of your required due date.

[*Insert company name*] will issue BlackBerry pagers to the help desk staff, who will then install it for the user.

It is the responsibility of each employee to use reasonable care in handling and protecting BlackBerry devices provided by the company, especially as corporate insurance policies cannot cover this type of loss. Should the BlackBerry equipment be lost, stolen, or damaged beyond repair, replacement costs must be borne by either the responsible employee or by the employee’s department at the discretion of the employee’s manager.

If you experience technical difficulties with a BlackBerry, you must report it to the tech support desk for assistance with troubleshooting and resolution. The support desk is trained in specific procedures to test and obtain replacement equipment. Be aware that replacement and/or repair may take XXX days to complete.

Protect your network from e-mail abuses

E-mail systems can be abused in ways that compromise or strain electronic communications resources. Every organization's e-mail policy should have provisions that forbid or limit such misuse.

Usages that can be a burden on system resources are:

- Perpetuating chain e-mail letters.
- Creating and sending spam.
- Sending or encouraging "letter bombs" that are used to harass others.
- Practicing an activity designed to deny the availability of electronic communications resources.

If your e-mail policy doesn't include prohibitions against these behaviors, insert the policy statement that TechRepublic has developed for you. Feel free to modify it to fit in with your organization's policy.

To produce this insert, TechRepublic has permission to use portions of polices from the following:

- The University of California
- The SANS Institute
- The Institute of Electrical and Electronic Engineers (IEEE)

TechRepublic recommends that you visit these sites to see the original policies used in producing the following e-mail use insert.

Unacceptable uses of e-mail are discussed in the Allowable Use section No. 7, "Interference," in the PDF version of the University of California's Electronic Communications Policy included in this download. Also included is IEEE's "E-mail Acceptable Use Policy." Both policies illustrate how an "unacceptable e-mail use" section should be included within an overall e-mail policy.

Unacceptable e-mail use: Interference

<Company name> forbids the use of company electronic communications resources for any purpose that could strain or compromise these resources. The company also forbids electronic communications that interfere with the use of these resources by other employees.

Toward this end, company resources may not be used to:

- **Perpetuate chain e-mail letters or their equivalents.** This includes letters that require the recipient to forward an e-mail to a specified number of addresses in order to achieve some monetary, philosophical, political, superstitious, or other goal. E-mails that are part of a multilevel marketing or pyramid-selling scheme, sometimes known as "Ponzi schemes," are illegal in many places and are specifically forbidden under this policy.
- **Create and/or send "spam."** Spam is defined as any unsolicited electronic communication that is sent to any number of recipients who did not specifically request or express an interest in the material advertised in the communication. It will be considered a greater offense if the company's electronic communications resources are exploited to amplify the range of distribution of these communications.
- **Send or encourage "letter bombs."** Letter bombs are extremely large or numerous e-mail messages that are intended to annoy, interfere, or deny e-mail use by one or more recipients.
- **Practice an activity designed to deny the availability of electronic communications resources.** Also called "denial of service attacks," these activities deny or limit services through mail bombing, malicious executables such as viruses, threatening a virus, or opening a large number of mail connections to a mail host or SMTP relay without authorization or permission.

IEEE E-MAIL ACCEPTABLE USE PRACTICES

The IEEE Acceptable Use Practices have been created to:

- Encourage the responsible use of resources (network, personal). Discourage practices that degrade the usability of network resources. Maintain the image and reputation of the IEEE as a responsible e-mail service provider.
- Protect the security, reliability, and privacy of IEEE's systems and network, and the systems and network of others, consistent with the policies of the IEEE.
- Safeguard the privacy and security of individual users, consistent with the policies of the IEEE

WHILE THE IEEE WISHES TO PROMOTE THE PRIVACY OF INDIVIDUAL MAIL USERS CONSISTENT WITH ITS E-MAIL POLICIES, THE IEEE CANNOT GUARANTEE THE SECURITY OR PRIVACY OF THE IEEES SYSTEMS AND NETWORKS OR THE NETWORKS AND SYSTEMS OF OTHERS. THE IEEE RESERVES THE RIGHT TO MONITOR E-MAIL USE TO ENSURE COMPLIANCE WITH ITS POLICIES. USERS SHOULD CONSIDER WHETHER IT IS APPROPRIATE TO USE E-MAIL FOR CONFIDENTIAL MESSAGES.

E-MAIL IS A PRIVILEGE, NOT A RIGHT. THE IEEE RESERVES THE RIGHT TO DISCONTINUE E-MAIL ALIAS OR E-MAIL LIST SERVICE, WITH OR WITHOUT WARNING, FOR ANY REASON INCLUDING, BUT NOT LIMITED TO, VIOLATIONS OF THIS POLICY. AN IEEE E-MAIL ALIAS DOES NOT AUTHORIZE THE RECIPIENT OR USER TO REPRESENT THE IEEE OR TO ACT ON BEHALF OF THE IEEE. THE IEEE RESERVES THE RIGHT TO MODIFY THIS POLICY AT ANY TIME, FOR ANY REASON DEEMED APPROPRIATE BY THE EXECUTIVE STAFF.

A USER MUST BEAR RESPONSIBILITY FOR HIS OR HER USE OF E-MAIL. THE IEEE CAN ACCEPT NO RESPONSIBILITY OR LIABILITY FOR ANY ACTIONS OF THE ALIAS RECIPIENT OR USER OR FOR ANY CONSEQUENCES RESULTING FROM USE OF E-MAIL, INCLUDING BUT NOT LIMITED TO, MISADDRESSED, LOST OR UNDELIVERED E-MAIL MESSAGES. THE IEEE WILL COOPERATE WITH AUTHORITIES CONDUCTING A LEGAL INVESTIGATION, OR OTHER OFFICIAL INQUIRY, INTO ILLEGAL ACTIVITIES OR UNLAWFUL ACTS ASSOCIATED WITH THE USE OF AN IEEE E-MAIL ALIAS OR E-MAIL SERVICE.

Users of IEEE e-mail aliases or mailing lists should be courteous to others when sending e-mail and should not abuse the service provided by the IEEE. Following is a non-exclusive summary of conduct that would be considered acceptable as well as unacceptable use of the IEEE e-mail alias and email list service:

Acceptable Use

Direct E-mail Communication to Members & Customers IEEE staff or volunteers who use e-mail for direct communications must have agreement from the member/customer that they will accept information via e-mail. The staff or volunteer must provide (or take advantage of an existing) mechanism for receiving this permission from the member or customer.

Direct e-mail communications covered may include, but is not limited to, the following:

- Informational announcements of new programs (e.g., GOLD activities, local seminars or events; Society, Section, Chapter, Region activities, Financial Advantage programs)
- Announcements regarding changes to programs, services (e.g., subscription info, terms and conditions)
- Fund-raising announcements (e.g., Life Member Fund, IEEE Foundation, History Center)
- New product promotions (e.g., books, standards, merchandise, subscriptions)
- Low cost/no cost inventory reduction promotions (e.g., net warehouse sale)
- Conference-related announcements (e.g., registration, call for papers, special activities, tour programs)
- Newsletters (an e-mail subscriber list is governed by the rules of IEEE e-mail list, as noted in policy procedures)
- Surveys (e.g., IEEE member survey, library survey, Society membership needs assessment)

This document should not be construed as a roadblock to the use of e-mail for person-to-person, the above or other communications.

Collecting Permission for Direct E-mail Communication

The member or customer should self-select as a target for direct e-mail communications. This can happen in a variety of ways including, but not limited to:

- Postcard announcement with response mechanism or other mailings to target member/customer group, asking for permission to communicate via e-mail.
- Toll-free number, message center or Website registration for members or customers where they may "sign up" to receive various types of communications electronically.
- "Welcome" or "appointment" letters or messages may incorporate this information.
- On-site conference registry for information related to that conference, etc.
- Via publications such as IEEE Spectrum, The Institute, etc.
- Via membership renewal, invoice or statement processes.

In certain cases, the nature of a volunteer or staff position, or participation in a specific group, may come with the caveat that (all or some) communications occur via e-mail. Once this is made clear to the individuals - either at the time of joining or as the policy of that specific group, activity or office changes - the electronic communication is appropriate and would fit these criteria.

Some Examples of Proper Usage

IEEE E-MAIL ACCEPTABLE USE PRACTICES

- Member requests that renewal information be provided electronically. IEEE provides that information via e-mail, at the e-mail alias or address on file.
- Section members request that information on local activities be provided via e-mail. These aliases are provided to the Section via SAMIeee program. Section announcements are provided electronically to the requesting Section member.
- Attendees at an IEEE conference are asked if they would like to receive future notices regarding similar conferences via e-mail. E-mail addresses or aliases are collected, and this communication is disseminated via electronic mail list.
- A print newsletter editor decides to "go electronic". Print subscribers (or recipients) are asked if they would prefer to receive the print or the electronic version, and their aliases or addresses are collected. The newsletter is sent via e-mail. Those receiving the electronic version do not need to be asked with each issue if e-mail is their preferred method.
- Members/customers asked - via online bookstore, response postcard mailing, conference signup or other means - if they would like to be kept informed of new titles in their field. Only print notices may be sent, unless the member/customer is specifically asked if they would like to receive such announcements electronically.

Unacceptable Use

- **Illegal Material**
  Do not send e-mail that contains any information that is illegal (e.g., copyright violations, trade secrets, and obscene material), harassing or threatening. Additionally, be aware that the transit of material into, or through, other countries may be required to comply with the law in that country. In some cases, this may include the transmission of encrypted messages
- **Chain Letters, Pyramid Selling, and Multi-Level Marketing Schemes**
  These are similar to the paper and mail-based letters that make these claims. Typical abuse of this sort includes the "Make Money Quick" scams. These not only waste resources, they are illegal in certain countries and may render the poster liable to prosecution.
- **Unsolicited External Commercial E-mail**
  Unsolicited external commercial e-mail, commonly referred to as spam, is advertising material sent without the recipient either requesting or denying receipt of such information or otherwise expressing an interest in the material advertised. Since many Internet users use a dial-up connection and pay for their online time, receipt of unsolicited external commercial advertising costs them money and is particularly unwelcome.
- **Electioneering**
  Using @ieee.org mailing list aliases for the purpose of promoting an election campaign is forbidden.
- **Confidential Material**
  It is inappropriate to send confidential information via e-mail since e-mail is not private and it can be read by anyone with the proper tools.

IEEE E-MAIL ACCEPTABLE USE PRACTICES

- **Unrequested Binary Messages**
  The majority of e-mail users are not able to select messages based on size and therefore such e-mails result in a significant waste of resources.
- **Forged Headers and/or Addresses**
  It is a grave abuse of the e-mail system if a message is sent that implies the sender can be contacted at an e-mail, postal, or fax address that is not under the direct control of the sender.
- **Electronic Mail Bombing**
  Electronic mail bombing is sending multiple e-mail messages, or one or more large e-mail messages, with the sole intent of annoying and/or seeking revenge on a fellow Internet user.
- **Resale or Commercial Use of Service**
  Your right to use the Service is personal to you. You may not allow any third person to use the Service. You may not resell or make any commercial use of the Service.

Due to the time taken to download it, sending long e-mail messages to sites without prior agreement can amount to denial of service, or it can create an inability to access e-mail at the receiving site. Note that if binary attachments are added to the e-mail, this may increase the size of the message considerably. If a prior arrangement has not been made, the mail will be extremely unwelcome.

Denial of Service Attacks

Denial of service is any activity that prevents a host on the Internet from making full and effective use of their facilities.
This includes, but is not limited to:

- Mail bombing an address in such a way to make Internet access impossible, difficult, or costly.
- Opening an unnecessarily large number of mail connections to the same mail host or making a connection to a SMTP relay (sometimes known as a smarthost) without authorization or permission.
- Sending e-mail designed to damage the target system when executed or opened; for example, sending malicious programs or viruses attached to an e-mail.
- Sending e-mail that is designed to cause confusion, consternation, fear, uncertainty, or doubt, such as fake virus warnings.

Mailing List Subscriptions

Never subscribe anyone other than yourself to a mailing list.
You must be aware of how to remove yourself from a mailing list in the event that you alter your e-mail address or discontinue your e-mail service.

If you have any further questions about the **IEEE E-mail Acceptable Use Practices**, please contact **email-aup@ieee.org**

A workplace safety policy for IT

Judging from a recent TechRepublic member survey, most companies do not have a safety policy that is targeted to address safety concerns of the IT staff.

Many companies use the general OSHA (www.osha-slc.gov/SLTC/ergonomics/) guidelines for workplace safety. The ARGroup (www.argroup.com) went a step further by creating a safety policy that includes specific guidelines for IT pros. This download also includes information steps that IT managers can take to improve health and safety issues for IT employees.

A policy example

The ARGroup, an IT consulting firm based in Leesburg, VA, is one of the few companies that has implemented a safety policy specifically addressing the dangers associated with IT. Brian Chavis, president of ARGroup, said the policy covers a wide range of safety issues (see Figure A).

FIGURE A

NO LEAN OVERs	IT personnel must sit down at the workstation they are fixing. The staff is not permitted to lean over computer users because over time, the constant bending may cause back problems.
NO TIES	Wearing ties is not allowed because the garment can get caught in equipment that's opened or get in the way of someone lifting, carrying, or setting something down.
NO REACHING DOWN INTO OPENED EQUIPMENT	Employees are trained on where the potential dangers are when opening equipment, such as a server, printer, or router. The sharp edges in these items can cause major cuts.
NO REACHING AROUND ELECTRICAL CONNECTIONS	The IT staff is encouraged to take items apart when working with electrical connections instead of reaching into an area that could cause an electrical shock. Reaching is especially tempting in tight quarters like data centers.
NO ONE CAN OPEN A MONITOR	Since monitors carry a large amount of electric volts, even when they're not plugged in, IT personnel are not permitted to open a monitor for any reason.
FAMILIARITY WITH GENERAL FACILITIES	Often, IT equipment is placed in odd locations—for instance, in power closets next to elevators. Employees must be educated on the non-IT systems and equipment that can pose electrical dangers in those areas. IT staff is also warned not to follow wires in these areas because the wires could cause an electrical shock or lead to something that will be dangerous. Asbestos in old buildings is another possible threat.
LIFTING	This is an increasing problem because equipment is getting heavier and larger. Employees are educated on the proper ways to lift and carry items. They are also advised not to carry heavy items (anything over 60 pounds) by themselves. Monitors should be carried with the tube, the heaviest area, toward the body, so the weight doesn't put added stress on the back.
STACKING	The IT staff is trained to place heavier equipment at the bottom of racks so there's not a top-heavy tipping problem.
WEAR A MOUTH MASK	If employees are opening equipment that has been in service for a long time, they should wear a mask over their nose and mouth to limit the exposure to large amounts of dust. Since many people are allergic to dust, it can cause sickness, which is a safety hazard.

Education is the foundation for safety

Safety experts said that education is the most important step in implementing a safety policy. "A company can spend the most money on expensive equipment, but if they never train their employees on how to use it correctly or at all, it's a waste of money," said Marc A. Yeager, a physical therapist and independent injury and management consultant in Atlanta.

Yeager frequently finds, for example, that employees complaining of back discomfort while sitting at a workstation don't need a new chair. They need to learn how to properly adjust their chair.

Here are some education topics that may improve safety in your department:

- How to properly use the equipment and tools
- How to self-treat an ache
- How to identify when an ache is significant and needs to be reported
- Appropriate body mechanics

Yeager said there are several principles of good body mechanics specific to the IT department. You may consider including these principles in your safety program:

- Lifting: Always use a good squat type of lift, bending with your legs, keeping your back in a neutral position. The same position should be used when lowering an item. Also, there is no set weight limit that is safe for everyone.
- Weight: Once you lift something, the bulk of the weight needs to be close to the body. The farther away the weight, the more stress on your back.
- Adding support: Many times, IT personnel have to get in awkward positions to connect cables in workstations or data centers. The forward bent position adds stress to the back. By simply putting one hand down on the work surface, while connecting cables, you help support the weight of your upper body.

Preventing repetitive-motion injuries

According to the National Safety Council, Carpal Tunnel Syndrome is the fourth costliest "nature of injury," averaging $11,944 per workers' compensation claim. Steve Skubish, assistant vice president of Loss Control at Atlantic Mutual Insurance Co. (www.atlanticmutual.com) in New York City, says the number of claims involving repetitive-motion injuries continues to increase. Just in the past eight months, Atlantic Mutual has received 130 claims, costing over $2.6 million in medical and legal expenses.

Making sure workstations are ergonomically correct for individual workers is the first step to controlling these injuries. This download also includes Atlantic Mutual's workstation checklist that you can use to help evaluate your staff's workspace and make recommendations for improvement.

Key responsibilities for the IT manager

According toYeager, the IT manager plays a key role in keeping employees safe and, as a result, limiting the expense of workers' comp claims. Yeager advises his clients to focus on finding a solution for each individual. "A lot of times, companies, especially large ones, will want that one quick fix," said Yeager. "They forget that we all have different body types. We have different job functions that don't always match."

Here's a list of key responsibilities for managers tackling IT safety:

- Empower employees to take breaks. OSHA generally requires a minimum of a 15-minute rest break at least every two hours.
- Encourage employees to report any discomfort or injuries. Make sure employees know that they are a greater resource to the company if they are healthy than if they're hurting or missing days of work. Also, make it known the pain could turn into something permanent if a change is not made in the environment or the injury is not treated.
- Know when to report an injury. Your company should have a policy on reporting injuries guided by OSHA recordables.
- Find individual solutions. Do not look for a quick fix. Each solution must be tailored to each individual based on physical attributes and job function.
- Get involved in the investigative process. Find out why an employee is hurting or injured and use the knowledge to build a personal database for solving similar problems in the future.
- Focus on buying electrical tools that limit a lot of repetitive wrist action. Furnish your staff with roller carts and tool belts.
- Encourage telecommuters to report discomfort and make sure their home workstations are ergonomically correct.

Workstation Checklist

Using this checklist is one way an employer or employees can identify, analyze and control Musculoskeletal Disorders (MSD) hazards in computer workstation tasks.

WORKING CONDITIONS

Yes No

A. Head and neck upright (not bent down/back). □ □

B. Head, neck and trunk face forward (not twisted). □ □

C. Trunk perpendicular to floor (not leaning forward/backward). □ □

D. Shoulders and upper arms perpendicular to floor (not stretched forward) and relaxed (not elevated). □ □

E. Upper arms and elbows close to body (not extended outward). □ □

F. Forearms, wrists, and hands straight and parallel to floor (not pointing up/down). □ □

G.Wrists and hands straight (not bent up/down or sideways toward little finger). □ □

H.Thighs parallel to floor and lower legs perpendicular to floor. □ □

I. Feet rest flat on floor or supported by a stable foot rest. □ □

J. Computer tasks organized in a way that allows employee to□ □ vary them with other work activities, or to take micro-breaks or recovery pauses while at the computer workstation.

SEATING

Yes No

1. Backrest provides support for employee's lower back (lumbar area). □ □

2. Seat width and depth accommodate specific employee (seat pan not too big/small). □ □

3. Seat front does not press against the back of employee's knees and lower legs (seat pan not too long). □ □

4. Seat has cushioning and is rounded/has "waterfall" front (no sharp edge). □ □

5. Armrests support both forearms while employee performs computer tasks and do not interfere with movement. □ □

KEYBOARD/INPUT DEVICE

Yes No

6. Keyboard/input device platform(s) stable and large enough to hold keyboard and input device. □ □

7. Input device (mouse or trackball) located right next to keyboard so it can be operated without reaching. □ □

8. Input device is easy to activate and shape/size fits hand of specific employee (not too big/small). □ □

9.Wrists and hands do not rest on sharp or hard edge. □ □

MONITOR

Yes No

10. Top line of screen is at or below eye level so employee is able to read it without bending head or neck down/back. □ □

11. Employee with bifocals/trifocals is able to read screen without bending head or neck backward. □ □

12.Monitor distance allows employee to read screen without leaning head, neck or trunk forward/backward. □ □

13.Monitor position is directly in front of employee so employee does not have to twist head or neck. □ □

14. No glare (e.g., from windows, lights) is present on the screen which might cause employee to assume an awkward posture to read screen. □ □

WORK AREA

Yes No

15. Thighs have clearance space between chair and computer table/keyboard platform (thighs not trapped). □ □

16. Legs and feet have clearance space under computer table so that employee is able to get close enough to keyboard/input device. □ □

ACCESSORIES

Yes No

17. Document holder, if provided, is stable and large enough to hold documents that are used. □ □

18. Document holder, if provided, is placed at about the same height and distance as monitor screen so there is little head movement when employee looks from document to screen. □ □

19. Palmrest, if provided, is padded and free of sharp and square edges. □ □

20. Palmrest, if provided, allows employee to keep forearms, wrists and hands straight and parallel to ground when using keyboard/input device. □ □

21. Telephone can be used with head upright (not bent) and shoulders relaxed (not elevated) if employee does computer tasks at the same time. □ □

GENERAL

Yes No

22.Workstation and equipment have sufficient adjustability so that the employee is able to be in a safe working posture and to make occasional changes in posture while performing computer tasks. □ □

23. Computer workstation, equipment and accessories are maintained in serviceable condition and function properly. □ □

PASSING SCORE = "YES" answer on all "working conditions" items (A-J) and no more than two "NO" answers on remainder of checklist (1-23).

For additional copies of this checklist, visit our website at www.atlanticmutual.com/losscontrol/ergonomics/checklist

Harassment and Disability Policy

1. Preventing Sexual Harassment

Title IX of the Education Amendments of 1972 prohibits sex discrimination against any participant in an educational program or activity that receives federal funds. The act is intended to eliminate sex discrimination in education. Title IX covers discrimination in programs, admissions, activities, and student-to-student sexual harassment. BYU's policy against sexual harassment extends not only to employees of the University but to students as well. If you encounter unlawful sexual harassment or gender-based discrimination, please talk to your professor; contact the BYU Equal Employment Opportunity Office at 422-5895; or contact the Honor Code Office at 422-2847.

2. Students with Disabilities

Brigham Young University is committed to providing a working and learning atmosphere that reasonably accommodates qualified persons with disabilities. If you have any disability that may impair your completing this course successfully, please contact the University Accessibility Center (422-2767). Reasonable academic accommodations are reviewed for all students who have qualified documented disabilities. Services are coordinated with the student and instructor by the UAC. If you need assistance or if you feel you have been unlawfully discriminated against on the basis of disability, you may seek resolution through established grievance policy and procedures. You may contact the Equal Employment Office at 422-5895, D-282 ASB.

FERPA Policy

What is FERPA?

The United States Congress passed the **Family Educational Rights and Privacy Act (FERPA)** in 1974 to afford certain rights to students concerning their education records. The primary rights afforded to students who attend a postsecondary school such as Brigham Young University are the right to inspect and review their education records, the right to seek to have their records amended and the right to have some control over the disclosure of information from the records.

Brigham Young University may not disclose information contained in education records without the student's written consent except under certain limited conditions.

FERPA Procedure

These procedures, in compliance with the Family Educational Rights and Privacy Act, (FERPA) govern access to student education records and identify the procedures students may follow to obtain or restrict access to their education records. These procedures are also designed to be in compliance with the Solomon Amendment which governs the rights of the military services to obtain student recruiting information. Individual academic departments and administrative areas may prepare their own policies and procedures consistent with these comprehensive university procedures.

The University Registrar is responsible for university compliance with these procedures. These procedures apply to the records of students who are both admitted and enrolled or who have previously attended the university on campus or via video conferences, satellite, internet, or by other electronic means. The rights are effective on the first day of the semester/term. They do not apply to applications of persons who were not admitted nor to other correspondence with the university.

EDUCATION RECORDS

These procedures apply to any education record (in handwriting, print, tapes, film, electronic or other media) maintained by BYU regardless of its date of origin which is directly related to a student. The following are NOT classified as education records under FERPA:

- Records kept by faculty, staff, administrative or auxiliary personnel for their own use as memory aids or reference tools if kept in the personal possession of the person who made them and the record has not been made available to any other person except the maker's temporary substitute. These personal notes are to be referred to in departmental and administrative records policies as "sole possession" records. Records that contain information taken directly from a student or that are used to make decisions about the student are not sole possession records
- An employment-related record which does NOT result from student status.

FERPA Policy

- University law enforcement records that are created and maintained by University Police for a law enforcement purpose.
- Parents' confidential financial statements, income tax records and reports received by the university.
- Records maintained by BYU health or counseling services that are used only for treatment and made available only to those individuals providing the diagnosis and treatment. Patient access to medical or counseling records is provided upon submission of written patient authorization according to university policy.
- Alumni records which contain only information about a student after he or she is no longer attending the university and do not relate to the person as a student.

ANNUAL NOTIFICATION

Student education records at BYU are generally accessible to eligible students according to the provisions of the Family Educational Rights and Privacy Act (FERPA). BYU has adopted Access to Student Records Procedures that explain in detail student rights relating to their education records. A copy of these procedures is available at the Office of the Registrar, B-150 ASB, Provo, Utah 84602-1114.

The following explains student rights to their education records, summarizes the procedures for exercising those rights, and describes student directory information that may be disclosed to the public without the students consent as required by law.

Eligible students, admitted and enrolled at BYU, generally have the right to:

1. Inspect and review their education records within a reasonable period of time upon submitting to the appropriate department managing their education records a written request, with proof of identification, specifying the records to be inspected. The department will notify the student of the time and place the records may be inspected.
2. Petition BYU to amend or correct any part of the education record believed to be inaccurate, misleading, or in violation of their privacy rights. Students may submit a written request to the department holding the record, clearly identifying the part of the record they want changed, and specify why it is inaccurate or misleading. If the department decides not to amend the record as requested, the department will notify the student of the decision and advise them of their right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures as outlined in university procedures will be provided to the student when notified of the right to a hearing.
3. Control the disclosure of personally identifiable information contained in the student's education record, except as otherwise authorized by law. Examples of exceptions to consent for disclosure include:
    - Access of education records by BYU officials and agents having a legitimate educational interest in the records. This category generally includes any BYU official or agent who accesses student educational records for the purpose of performing a task or responsibility relating to his or her employment or professional responsibility at the university. These individuals may include

faculty, administration, staff and other university agents who manage student education record information including, but not limited to, student education, discipline, and financial aid.

  - Parents who establish the student's dependency for federal income tax purposes.
  - Upon request, BYU will disclose education records or information without consent to officials of another college or university to which the student seeks or intends to enroll, or to a school in which the student is currently enrolled.

4. File a complaint with the U.S. Department of Education concerning failures by BYU to comply with the requirements of FERPA. The name and address of the office that administers FERPA is: Family Policy Compliance Office, U.S. Department of Education, 400 Maryland Avenue SW, Washington, D.C. 20202-4605.
   www.ed.gov/offices/om/fpco/

DIRECTORY INFORMATION

BYU has designated the following student information as directory information that it **may** disclose to the public without the consent of the student:

- Name
- Addresses and telephone numbers
- E-mail address
- Month, day and place of birth
- Names of parents or spouse
- Major and minor fields of study
- Participation in officially recognized activities and sports
- Weight and height of members of athletic teams
- Pictures
- Dates of attendance (current and past)
- Number of months/semesters enrolled
- Class standing (freshman, sophomore, etc.)
- Enrollment status (full-time, part-time, less than half-time)
- Degrees and awards received
- Previous educational institutions attended
- Dates of employment and job title for student employment positions
- Anticipated future enrollments
- Course registrations prior to the beginning of a semester/term
- Expected date of graduation
- Deferred registration eligibility

Students have the right to restrict disclosure of the above directory information. To request restriction of disclosure, students must file a written request in the Registrar’s Office. To avoid being listed on some directories, this must be done on or before the tenth day of a semester or the sixth day of a term and will remain until the student specifically rescinds the restriction.

Directory information is not provided to third parties in the form of mailing lists or labels.

FERPA Policy

Departments or colleges requesting mailing list information or other directory information may do so by contacting the Registrar's Office. Departments or colleges should provide a written request with the signature of the dean, department chair, or director explaining the need for the information and how it will be used.

Restricting Academic Records

The University determines the personal information regarding its students that can be given to the public upon request according to the FERPA guidelines. Any Brigham Young University student can request to restrict the disclosure of this personally identifiable information by the following procedure:

1. Come to the Records Office in B-150 ASB with personal identification
2. Request a restriction be put on his or her academic records
3. Fill out and sign the written agreement provided

To remove the restriction on education records, a student should bring proof of identification to the Records Office and request that the restriction be taken off of his or her records.

Any contact with our office or other departments on campus can *only* be done in person or in writing.

The above processes are completed through the University Registrar for the protection of the students and to be in compliance with FERPA.

MILITARY RECRUITERS AND THE SOLOMON AMENDMENT

BYU supports and complies with the Solomon Amendment. Requests for student recruiting information from military recruiters are made with the Registrar's Office. Student recruiting information will not be supplied with respect to students who have not reached the age of 17. Additionally, if a student has formally requested BYU to withhold FERPA directory information from third parties, BYU will withhold this information from military recruiters as well. This file will contain all students enrolled in day school for the year term in which the request is made. The file will contain the following information: name; street; city; state; zip; telephone; birth date; class standing; department; major; emphasis; first degree from BYU; degree name; degree year; second and third degrees from BYU by name and year, last college/university attended; credit hours; citizenship; email, and anticipated graduation date.

LOCATIONS OF STUDENT EDUCATION RECORDS

The following list describing the type, location and custodian of university student education records is illustrative and not comprehensive. Other student education records may be found in a variety of locations throughout campus. A student having questions concerning the location of education records should direct an inquiry to the applicable department or college.

FERPA Policy

TYPE	LOCATION	CUSTODIAN
Admissions, Registration, Records, and Graduation Evaluation Services	B-150 ASB	Registrar
Student Life	3500 WSC	Dean of Student Life
Honor Code	4440 WSC	Director of Honor Code Office
Academic Support	2500 WSC	Director of Academic Support
Financial Aid	A-41 ASB	Director of Financial Aid
Housing	100 SASB	Director of Housing
Placement Center	2400 WSC	Director of Placement
Progress Reports, Graduate Admissions	Dean's Office or Student Advisement Center of each College or Department	Dean or Student Advisement Coordinator
Faculty Records	Faculty Office at each College or Department	Instructor
Law School	341 JRCB	Law School Records Custodian
Graduate Studies	105 FPH	Dean of Graduate Studies
Occasional Records (student education records not included in the types listed above.)	The appropriate official will collect such records, direct the student to their	University personnel who maintain such occasional system records.

	location, or otherwise make them available for inspection and review.	

PROCEDURE TO INSPECT EDUCATION RECORDS

FERPA controls access to student education records. BYU will make a reasonable effort to provide eligible students and qualifying parents the rights granted by the Act. On presentation of appropriate identification and under circumstances that prevent alteration or mutilation of records, a student with proper identification will be permitted to inspect all education records not restricted by a pledge of confidentiality or considered to be private records of university personnel. In those instances when the university is willing to allow copies, those with legitimate access to the records will be charged a reasonable fee for the copies.

Students are encouraged to submit to the record custodian or to appropriate university personnel a written request that identifies as precisely as possible the record the student wishes to inspect. However, oral requests may be honored upon proper presentation of identification and in circumstances where a written request would be burdensome or impractical.

The record custodian or appropriate university personnel will make reasonably prompt arrangements, generally within 45 days, for access and notify the student of the time and place where the records may be inspected.

When a record contains information about more than one student, the student may inspect and review only that portion relating to the requesting student.

RIGHT OF UNIVERSITY TO REFUSE ACCESS

The following records are not available for review by students:

- The financial statements and tax returns of the student's parents.
- Letters and statements of recommendations to which the student has waived the right of access, or which were placed in the student's file before January 1, 1975.
- Records connected with an application to attend BYU or a component unit of BYU if that application was denied.
- Any records which are not education records as defined by FERPA or these procedures and which are not otherwise accessible pursuant to law.

REFUSAL TO PROVIDE COPIES

BYU reserves the right to deny transcripts or copies of education records if:

- The student has an unpaid financial obligation to the university;
- The student is in default under any federal loan program,
- There is an unresolved disciplinary action against the student;

- There is unresolved litigation between the student and the university;
- The student has failed to comply with the decision of the arbitrator(s) under the Arbitration Rules of the BYU Center for Conflict Resolution; or
- Other cases as determined by the university procedures on Registration and Academic Holds;
- Or as otherwise determined appropriate by the university.

BYU will not provide copies of those education records related to disciplinary action taken against a student, even at that student's request, unless refusal of such a request would unreasonably limit the student's right to inspect and review those records.

COPIES OF RECORDS

If for any valid reason such as work hours, distance from a student's place of residence to a record location, distance between record location sites, or health, a student cannot inspect and review his or her education record in person, BYU may arrange for the student to obtain copies. A reasonable fee for copies and any applicable postage fees will be charged. The fee for copies at the Office of the Registrar will be $.50 per page unless otherwise specified. There is no charge for search or retrieval of education records nor for personal inspection of education records.

DISCLOSURE OF STUDENT EDUCATION RECORDS

BYU will disclose student education records to a third party with written consent from the student. This written consent must:

- Specify the records to be released,
- State the purpose of the disclosure,
- Identify the party or class of parties to whom disclosure may be made, and
- Be signed and dated by the student.

BYU will disclose student education records without the written consent of the student in the following limited circumstances:

- To school officials and to specified agents of the university who have a legitimate educational interest in the records.
  - A school official or specified agent of the university is:
    - a member of the Board of Trustees; or
    - a person employed by the university in an administrative, supervisory, academic, research or support staff position, (including law enforcement unit personnel and health staff); or
    - a person or company, with whom the university has contracted as its agent to provide a service instead of using university employees or officials (such as Student Clearinghouse, an attorney, auditor or collection agent); (the contracted party is subject to the same conditions of use and redisclosure of education records that govern other school officials); or

        - a student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks; or
        - a person employed by, under contract to, or designated by the university to perform a specific task.
    - A school official or specified agent has a legitimate educational interest if the official is:
        - performing a task that is specified in his or her position description or by contract agreement;
        - performing a task related to a student's education;
        - performing a task related to student discipline; or
        - performing a service or benefit relating to the student or the student's family, such as health care, counseling, job placement or financial aid.
    - To officials of another school, upon request, in which a student is enrolled or seeks or intends to enroll.
- To the Secretary of the U.S. Department of Education, the Attorney General of the United States, the Comptroller General of the United States, and state and local educational authorities, in connection with certain state or federally supported education programs.
- In situations where a student has sued the university, or the university has taken legal action against a student, as necessary for the university to proceed with legal action as a plaintiff or to defend itself.
- In connection with a student's request for or receipt of financial aid, as necessary to determine the eligibility, amount or conditions of the financial aid, or to enforce the terms and conditions of the aid.
- As required by state law disclosure that was adopted before November 19, 1974.
- To organizations conducting certain studies for or on behalf of the university on condition that the organizations conducting the studies not permit the personal identification of students by anyone other than the organizations' representatives. Additionally, all information provided must be destroyed by the requesting organizations when no longer needed for the study’s purposes.
- To accrediting organizations to carry out their functions.
- To either parent of an eligible student if the student is claimed as a dependent for income tax purposes regardless of which parent claims the student as a dependent. Parents requesting information from a student's file shall be responsible to demonstrate that the student in question is a dependent pursuant to Section 152 of the Internal Revenue Code. In addition, BYU may disclose to parents of an eligible student information regarding violations of local, state or federal law or of the Church Educational System Honor Code regarding the use or possession of controlled substances for student violators under the age of 21.
- To comply with a judicial order or a lawfully issued subpoena in which case the order or subpoena shall be directed to the Office of the General Counsel for review prior to dissemination of the education record. The university will make a reasonable attempt to notify the student in advance of disclosure when non-directory information is released in response to subpoenas or court orders.
- To appropriate parties, including parents or guardians, in a health or safety emergency.

FERPA Policy

BYU may (without the consent of the perpetrating student) disclose to the victim of a crime of violence or a sex-offense, (as defined in the Clery Act) the results of any disciplinary proceeding conducted by BYU against the alleged student perpetrator regardless of the outcome of the proceeding.

Upon request, information received from the state of registered sex offenders pursuant to the Campus Sex Crime Prevention Act Amendment to the Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act who are employed, carry on a vocation, or who are students enrolled at BYU will be made available to the requesting party.

RECORD OF REQUEST FOR DISCLOSURE

Each custodian of education records at BYU will maintain a record of all requests for and disclosures of information from a student's education records file made by anyone other than a school official or the student. The record will indicate the name of the party making the request and the reason for the release. The record of the request for disclosure may be reviewed by an eligible student.

Redisclosure of education records by a third party is prohibited.

CORRECTION OF EDUCATION RECORDS

Students have the right to ask to have education records corrected that are inaccurate, misleading or maintained in violation of their privacy or other rights. In cases of alleged academic dishonesty or of an unfair or mistaken evaluation, the students must pursue redress under the Student Academic Grievance Policy. In cases of alleged violations of the Church Educational System Honor Code, the student must pursue redress under the applicable policies and procedures of the Honor Code Office. In cases of other non-academic, extenuating circumstances or emergencies potentially affecting a student's education records, students must pursue redress through BYU's Student Academic/Registration Record Appeals Committee. In all other cases of challenge to the content of a student's education records, not otherwise governed by established university policy, these procedures will apply. Under these procedures, the process must be initiated within one year from the semester or term in question. The following are the applicable procedures:

- A student must file a written request with the custodian of the applicable BYU education record to amend the record. The request should identify the part of the record requested to be changed and specify why the student believes it to be inaccurate, misleading or in violation of the student's privacy or other rights.
- The dean or supervisor of the university area maintaining the records shall promptly review the facts and seek to resolve the complaint by informal discussions with the student.
- If the dean or supervisor decides not to comply with the request, BYU will notify the student in writing.
- A student who disagrees with the decision has a right to a hearing to challenge the information believed to be inaccurate, misleading or in violation of the student's rights.

Upon written request to the University Registrar, a hearing will be scheduled and the student will be provided reasonable advance notification of the date, place and time of the hearing. The hearing will be conducted by the University FERPA Committee consisting of three disinterested individuals appointed from the Office of the Dean of Students and the Office of the University Registrar or another appropriate custodian of the student education records. The student shall be afforded a meaningful opportunity to present evidence relevant to the issues raised in the original request to amend the student's education records. The student may have one or two individuals, physically present at the hearing panel to confer with him or her. Because the hearing is not intended to be adversarial, however, such individuals will not be allowed to address the hearing panel nor advocate, unless specifically invited to do so by the Chair. The hearing panel will be advised on matters of procedure and law by the Office of the General Counsel. The hearing panel will prepare a written decision based on the evidence presented and/or considered at the hearing. The decision will include a summary of the evidence and the reasons for the decision.

- The hearing panel will strive to ascertain the truth and to make determinations that are reasonably supported by the evidence. Note: this hearing is an administrative proceeding and no attempt shall be made to apply the formal rules of evidence applicable in judicial proceedings. In general, any evidence, whether oral testimony or documentary, which is considered by the hearing panel to be relevant should be received subject to the discretion of the hearing panel to exclude frivolous, repetitive or merely cumulative testimony.
- If the hearing panel finds that the information is not inaccurate, misleading or in violation of the student's right of privacy or other rights, the record will be maintained, but the student will be notified of the right to place in the record a statement commenting on the challenged information and/or a statement setting forth reasons for disagreeing with the decision. The statement will be maintained as part of the student's education records as long as the contested portion is maintained. If BYU discloses the contested portion of the record, it will also disclose the statement. If the hearing panel decides that the information is inaccurate, misleading or in violation of the student's right of privacy or other rights, it will amend the record and notify the student, in writing, that the record has been amended.
- Generally, the university will follow the procedural guidelines as outlined above. However, the procedures set forth above are merely guidelines and are not intended to create any contractual obligations or expectations. The university reserves the right, at its reasonable discretion, to vary these procedures according to the circumstances of individual matters, provided that the student is not significantly prejudiced.

INTERPRETATION

Questions concerning the application of these procedures should be addressed to the Office of the Registrar, B-150 ASB, Provo, UT 84602. The Registrar, in consultation with the BYU Office of the General Counsel, will determine all questions of interpretation.