Insulation Supply Company

Employee Computer Use Policy

Revision A – Released 6/15/2001

Approved By Mark Blumenfeld – General Manager

Scope

This policy applies to all computer, voice and data equipment owned or leased by Insulation Supply Company, Incorporated at all corporate locations.

If, at any time, all or any part of this conflicts with Federal, State or Local laws, the laws shall supercede this document. If any of this document is superceded by applicable law, the remainder of this policy shall remain in effect.

This policy applies to YOU! It is your responsibility to read and understand all sections of this document. If you need help in understanding or interpreting any part of this policy, please see a manager for clarification.

Table of Contents

Employee Computer Policy

Purpose

The purpose of the Employee Computer Operating and Security Policy is to help protect the company and employees of the company from liability and business interruptions due to inappropriate use of company computers and breaches of computer security.

This policy documents the computer users' responsibility to safeguard computer equipment and information from accidental or deliberate unauthorized access, tampering, snooping, distribution, or destruction. It sets forth what is, and is not, appropriate use of company computers. Users may be disciplined for noncompliance with company policy. This policy does not purport to address every computer operating and security issue. It is your responsibility to use sound judgment. Should you identify an issue or situation that you are not certain how to deal with, inquire of management.

The Employee Computer Operating and Security Policy is subordinate to any collective bargaining agreement, employment contract, or other employment agreements. The company may add to, or change, the policies at any time. Please read the policy carefully and sign the ***Receipt of Employee Computer Operating and Security Policy*** form attached. The signed form should be given to your supervisor for placement in your personnel file.

Introduction

In the early days when computers were centralized and managed by data centers, using the computer was very different. Computers were housed in cold rooms with big padlocks and only computer technicians, and other authorized personnel had access. Links to the outside world were unusual, and the purpose of the computer was principally for computing. In addition, and more importantly, while some very important systems were maintained on these computers, they represented only a few systems such as accounting, payroll, billing, and the like. Computers did not house every single aspect of our work life, from our most important, confidential documents and worksheets, to our daily communications and calendar.

Portable and desktop computers have changed all that. Today, many people have access to computers. With the continuing increase in the power of computers, and the number of employees using computers, the time spent on computers can only increase. Because so much important work is stored on computers, and computers are used for transmission of company records, it is important that management provide guidance on proper use of company computers.

The impact of the computer on our business has been significant, and at breakneck speed. The technology accessible today could not have been speculated just five or ten years ago. Who knows what we will have available to us in a few more years. Keeping technology current is key to our competitiveness, and provides unprecedented opportunity for the company and its employees to succeed. In that same vein, it puts us at considerable risk. Implementing new technologies is expensive, time consuming, and without established policies and practices in place, could lead to disaster. We do not have to look very far to find numerous examples of large companies that have incurred substantial losses due, in part, to the computer.

The first, best, and most important line of defense starts with our people!

It is unquestioned that a well-trained work force properly versed in computer operating procedures, and computer user security matters, will have the best chance of minimizing business interruptions due to inappropriate, negligent, or unethical use of company computers. For this reason, we have created Employee Computer Operating and Security Policy. Please understand it is not our intention to encumber your use of the computer, but rather our fiduciary responsibility to protect the resources of the company. We believe this policy accomplishes that with little to no hardship to you, the computer user and our valued employee.

Employee Computer Operating and Security Policy

Computer Users

Computer users are responsible for the appropriate use of company computers, and for taking reasonable precautions to secure the information and equipment entrusted to them. Employees are responsible for reporting inappropriate use of company computers, and breaches of computer security, and assisting in resolving such matters. Users are responsible for adhering to company policies and practices as described herein, and in other company policy manuals, to ensure company computers are used in accordance with company policy guidelines, and reasonable measures are taken to prevent loss or damage of computer information and equipment.

Unauthorized Access

Unauthorized access of company computers is prohibited. Unauthorized access of third-party computers, using company computers, is prohibited. Attempting to access company computers without specific authorization is prohibited. Any form of tampering, including snooping and hacking, to gain access to computers is a violation of company policy, and carries serious consequences. Employees are required to turn their computer off at the end of the day, and when not in use for an extended period of time. This will help prevent computer security breaches, and damage due to power surges. In addition, computer users must take other reasonable precautions to prevent unauthorized access of company computers.

Computer Sabotage

Destruction, theft, alteration, or any other form of sabotage of company computers, programs, files, or data is prohibited and will be investigated and prosecuted to the fullest extent of the law.

Passwords

The fox is in the hen house.

Dr. Thomas Longstaff of the CERT Coordination Center (CERT/CC) at Carnegie-Mellon University wrote, "Simple password guessing is still the most prevalent and effective method of system penetration." CERT/CC estimates that 80 percent or more of the problems they see have to do with poorly chosen passwords.

If poor password selection is not enough, according to *The Underground Guide to Computer Security by Michael Alexander, most computer crimes are committed by current and former employees.*

This means the individuals that have the greatest access to information to crack your password, are the same individuals that are committing most of the computer crimes.

The examples above are provided to demonstrate how crucial your participation is to effective computer security. Not only the company is at risk when someone gets your password. Computers often contain confidential information. If this information is accessed and distributed, it could cause great harm to you or someone you work with. Once someone gets your password, they have the capacity to, among other things:

- Send e-mail to individuals, or groups, representing themselves as you
- Disseminate your files over the Internet
- Delete or alter files
- Share your password with other interested parties
- Monitor your work

There are bulletin boards on the Internet where passwords are traded and exchanged for credit card numbers and other items considered of value. If a hacker gets your password, it most likely will be used to access more vital computer systems where much more damage can be done.

Password Selection and Protection

Select difficult passwords. Change them regularly, and protect them from snoopers. A lot of damage can be done if someone gets your password. Users will be held accountable for password selection and protection.

Do not share your password with anyone, other than a designated company official. Do not write it down where someone can find it, do not send it over the Internet, Intranet, e-mail, dial-up modem, or any other communication line.

Poor password selection and safekeeping is not comforting to management investigating a computer security breach, nor is it an acceptable excuse if a hacker damages company computer systems using your password.

Password Cracking

It is not uncommon for employees to try to figure out a friend's, or associate's, password, just to see if they can. However, the same employee would never steal the key and go through your desk drawer, looking at everything and anything private and confidential. Yet, this is just what happens when passwords are cracked. Stay away from such activity. It is a serious violation of company policy.

Easy to Remember and Hard to Crack

Another concern is forgetting your password. Getting into your computer when you have forgotten the password is, in some cases, very difficult. A good method to help you remember your password is to select passwords that are unique to you, and try to use it at least once every day. For example, if you live on Elm Street, do not select "elm" as a password. Select the nearest crossroad and always finish, or start, with a number (maybe your youngest child's age).

The following is a good guideline for password selection:

- Use 5 or more characters, and at least one alphanumeric character
- Your password should not include your login name, your name, your spouse's or partner's name, children's or pet's name, or any other names commonly known to others
- Your password should not be a word pertaining to the company, your work, or an activity that you participate in or follow that is commonly known
- Your password should not include anything derogatory, offensive, or defamatory

If you have a question about password selection or safekeeping, please see your supervisor or the Information Systems Manager.

Password Access Program

The company's password access program is an excellent tool to defend against unauthorized access of company computers. However, a password access program is only effective when used properly.

Do not leave your computer logged on and unattended for an extended period of time. Do not log on to your system if someone can see you keying in your password

(there is no need to create the temptation). Make sure the password access program is set to deny access to your computer after three unsuccessful attempts (this makes it difficult for someone using a program designed to crack passwords to successfully access your computer). Report any irregularities flagged by the password access program (last login time and date, number of attempts to login, etc.). Turn off your computer when you leave at night. If you use a remote access program, and you need to leave your computer on, be sure that it is in a locked room. Furthermore, use a screen saver access program to secure the computer from unauthorized access.

Snooping

Snooping -- an affectionate term common in the English language. Defined in Webster's Dictionary as "to pry about in a sneaking way."

Snooping into company computer systems is a serious violation of company policy. If you have no business being there, don't go there. If you accidentally identify a new way to access information, report it to management. Watching other users enter information, and looking at computer disks that do not belong to you, are prohibited. Obtaining, or trying to obtain, other users' passwords, or using programs that compromise security in any way, are violations of company policy. If you observe someone snooping, report it to management.

Hackers

Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network *was among Macmillan Computer Publisher's top 20 sellers on its computer list in 1997. Not only are the techniques for hacking into computer systems discussed in great detail, but also the author provides a CDROM with the tools to help accomplish computer crimes.*

Books like the one above, and there are many, provide the knowledge to make most anyone competent at bypassing computer security systems. Accordingly, it takes a concerted effort by all employees to maintain secure computer systems.

Hackers are working hard to break into computer systems. They alter and delete files, and cause other havoc for fun or profit. A common exposition of hackers prosecuted for criminal activity is that they felt computer systems' weaknesses exist to be exploited. This is the mentality we are dealing with. Very smart people with little or no common sense, and clearly too much time on their hands.

Hackers frequently penetrate computer systems by calling unsuspecting employees representing themselves as a new employee, executive of the company, or another

trusted individual. Through a variety of probing questions, they obtain the information necessary for their hacker programs to do their work.

Never give any information about computer systems out over the telephone, or in any other way. If someone requests such information, get their name and phone number, and tell them you will get right back to them. Report the incident immediately to management. Without your help, the company has little chance of protecting the company's computer systems.

Using hacker programs and trying to access computer systems using hacker techniques is prohibited. Trying to hack into third party computer systems using company computers is prohibited, and will be reported to the local authorities. Hacker crimes result in millions of dollars of downtime, lost data, and other problems. If you are caught hacking, it is a serious offense. If you identify vulnerability in the company's computer security system, report it to management.

Viruses, Worms and Trojan horses

The ICSA, Inc., Computer Virus Prevalence Survey, found that the rate of virus infection in 1998 is 48 percent higher than in 1997. According to the study, diskettes are still the most common route of infection. However, e-mail and the Internet are rapidly growing sources of viruses. InformationWeek magazine.

It is critical that users make certain that data and software installed on company computers are free of viruses. Data and software that have been exposed to any computer, other than company computers, must be scanned before installation. This includes e-mail with attachments (a virus can quickly contaminate your computer simply by opening an e-mail attachment), downloads form the Internet and other sources of data that may be contaminated. Viruses can result in significant damage, and lost productivity. If you are uncertain whether data or software needs to be scanned before installation, see the Information System Manager.

Use of virus, worm, or trojan horse programs is prohibited. If you identify a virus, worm, or trojan horse, or what you suspect to be one, do not try to fix the problem. Immediately turn your computer off, make notes as to what you observed, and contact the Information Systems Manager. The principal concern is stopping the contamination before additional damage is done. These programs are most successful when ignored. They are designed to easily hop from application to application, contaminate a computer disk, and access another computer. They easily travel down phone, cable, ISDN, or other communication lines, infect e-mail, data and files, and find their way to other computer systems. The key to containment is limiting the reach of the contamination. Turning off your computer does this best.

Confidentiality

General

All computer information is considered confidential unless you have received permission to use it. Accessing or attempting to access confidential data is strictly prohibited. Confidential information should only be used for its intended purpose. Using confidential information for anything other than its intended use is prohibited, without prior management approval.

Handling Confidential Information

Confidential information stored on computers is typically more difficult to manage than traditional paper documents that are sealed in an envelope, and locked in a filing cabinet clearly labeled CONFIDENTIAL. As such, it is important that users take extra care with confidential information stored on computers. The following are inappropriate under normal circumstances when dealing with confidential information:

- Printing to a printer in an unsecured area where documents may be read by others
- Leaving your computer unattended with confidential files logged on to your system
- Leaving computer disks with confidential data unattended, in easy to access places. Remember it only takes a minute to copy a disk
- Sending confidential information over the Internet, Intranet, dial-up modem lines, or other unsecured communication lines without approval from departmental management and information systems management

If you observe a document at a shared printer, or any other location, do not read it without permission.

Encryption

Encryption and encryption utilities are prohibited without management approval. If you need to send confidential or proprietary information over the Internet, or other public communication lines, you must obtain prior approval from management.

Physical Security

Computer Theft

The following is an excellent example of a physical security breach as reported in COMPUTERWORLD magazine:

A laptop stolen from the British Defense Ministry in the early 1990's had the entire Desert Storm war plan on it. The theft caused a furor among NATO allies. It is believed the data was never used but rather the machine was stolen for the hardware.

The data stolen may be backed-up. However, as shown in the example above, back up may not be the biggest concern.

Locks

Physical security is key to protecting your computer and computer information from loss and damage. Store floppy disks and other sensitive information in a locked drawer. Turn off your computer when it is not in use for an extended period of time. Lock the door to your office, if you have one. Take a few minutes to practice good physical security. Your investment of time will provide an excellent return, and help prevent temptation by others.

Laptops

There is no sure way to secure laptops. However, there are many sensible, cost-effective measures that can help reduce the risk of loss or damage. The following are required when taking laptops off company property:

- Laptops must be signed out with the information systems department
- Report lost or stolen computers immediately
- All important files must be backed-up, and back-up disks must be stored in a separate physical location from the computer
- Confidential, important, and proprietary data leaving the facility requires management authorization
- Use reasonable precautions to safeguard the laptop against accidental damage (don't work on your laptop in the pool)
- When traveling, laptops must be in sight at all times or physically secure
- Always store laptops in a concealing carrying case

Off-Site Computers

Off-site users must take additional precautions to safeguard computer information and equipment, including but not limited to:

- Safeguarding the computer and information from theft or damage
- Prohibiting access to the computer (including family, friends, associates, and others) for any purpose, without management authorization
- Adhering to all computer policies and practices of the company for on-site users

Administrative Matters

Back-up

Only you can prevent data loss!

Users are responsible for regular back up of essential computer files, and secure storage of back-up disks. It takes about four hours to replace a computer. With proper back-up practices, it should take about the same amount of time to replace the data.

Backing up files is key to productivity, and safeguarding data against unwanted intrusions. Important files should be backed-up daily. Decisions about what to back up, and how often to back-up, should be considered with one simple thought in mind. How much productivity would be lost if your computer were stolen? So much work is done in a single day, that in most cases, it is irresponsible to not take a few minutes to back-up essential data. The stories of individuals losing a day, a week, a month, or more of work are endless. Data will be lost. Eventually, it happens to everyone. The only question is, how much?

All backed-up files should be stored on a secure computer disk or tape, other than the one containing the original data. The back-up disk or tape should be stored on site, preferably in a locked drawer.

All important, confidential, or proprietary information must be stored on the local area network (LAN). Storing information on your desktop computer is prohibited without authorization from management. The LAN is equipped with electronic and physical security. Activity on the network is monitored for tampering, and other security breaches. Maintenance and back up are performed on the LAN daily. Programs and other information are updated on the LAN regularly. Use the LAN; it is safe, effective, and reliable.

Copyright Infringement

The company does not own computer software, but rather licenses the right to use software. Accordingly, company licensed software may only be reproduced by authorized company officials in accordance with the terms of the software licensing agreements. Unauthorized copying, redistributing, and republishing of copyrighted or proprietary material are strictly prohibited. Copyright laws apply on the Internet as well. There is no “but copying it was so easy” defense to copyright infringement. Copyright infringement is serious business, and the company strictly prohibits any such activity. If you have questions about copyright infringement, discuss it with management immediately.

Copies of shareware or “free” programs must be registered with the information systems department. Shareware and free software often have licensing and use restrictions, and should not be copied or forwarded to others. Typically, if you continue to use shareware you must send in a “donation,” often of a specified amount. If you neglect to do so, you may have committed copyright infringement. If you provide the program to a friend, you may have violated copyright law. It is not unusual for “free” software to contain a virus. As such, it is important that all new software is registered with the information systems department. Your supervisor and the Information Systems Manager must approve requests for application programs.

Harassment, Threats and Discrimination

It is company policy, and the law, that employees are able to work free of unlawful harassment, threats, and discrimination. Unlawful harassment is physical or verbal behavior directed towards an individual due to their race, age, marital status, gender, disability, religion, sexual orientation, or nationality for the purpose of interfering with an individual’s work performance, or creating an intimidating or hostile work environment.

It is not uncommon for employees to receive files, data, pictures, games, jokes, etc., that may be considered offensive by some. Currently, there are many cases in the courts addressing just such issues, the ramifications of which are significant. The computer is possibly the easiest tool for obtaining, storing, sharing, and disseminating to large audiences such material and viewpoints. Stay away from such activity; it is a serious violation of company policy. It is inappropriate to use company computers to share your personal views about religion, politics, sexuality, or any other subject of a personal nature that could be œnsidered offensive to others within or outside the company. Company computers are not vehicles to express free speech. Do this on your own time, away from the company, using your own resources.

We do not have to look very far to find numerous examples of individuals that do not understand the seriousness of sexual harassment. The following is just one such example:

In 1995, Chevron Corporation paid more than $2 million to four female employees to settle their claim that they were harassed by sexually explicit e-mail messages, including "25 reasons beer is better than women." COMPUTERWORLD magazine.

Computers provide a huge potential for unlawful harassment. Users often think their communications are private, and trashed or deleted files are gone forever. However, deleted files are often easily recovered; and information on company computers is not necessarily private. Users often feel comfortable writing and storing files within the confines of their "personal" computer, and sharing personal views on a wide range of non-business subjects. Remember, whatever you transmit is a permanent record to the receiver. It can, at some future date, be taken out of context and used against you and the company.

Accidents, Mistakes and Spills

We have met the enemy and he is us. Pogo

It is not hackers, snoopers, viruses, worms, or trojan horses that cause the most damage to computers and information. It is, by far and away, us, the computer users. According to current research, most data loss and damage to computers is done by authorized users. Mistakes and accidents represent the biggest cost when it comes to computer information loss. We have all done it, deleted a file that we just spent hours creating, spilled coffee on the keyboard, or dropped the laptop on the floor.

"*An ounce of prevention is worth a pound of cure"* is a very appropriate cliché for computer operations. Take a few seconds to read the computer screen before you delete, save, or transmit files. In addition, users need to take reasonable precautions with respect to computer operations, maintenance, handling, and transportation. It is not our intention to prohibit coffee at your desk. However, when placing liquids, and other food items on your desk, please be careful.

Unauthorized Changes to Company Computers

Have you seen the sign at the automobile mechanics garage?

Labor rate is $50.00 per hour. If you already worked on the car, $75.00 per hour. If you help, $100.00 per hour.

Installing software and making changes to computer hardware, software, system configuration, and the like are prohibited, without management authorization. The company's computer systems have been designed and documented to prevent loss of data, and provide an audit trail for correcting problems. Unauthorized changes to computer systems ultimately result in lost productivity. Such changes often require a computer technician to fix both the original problem, and the problem caused by the would-be computer technician. Poor documentation of the procedures performed, and the order in which they were completed further complicate unauthorized changes to computer systems.

The following are just a few examples of changes to computers that can result in operating problems:

- Installation of commercial software, shareware, and free software. Some software requires an upgrade of computer hardware, the operating system, or both for the program to operate properly. Some programs are simply not written well, and can cause problems with the computer
- Installation of some programs changes the computer's system configuration, which can result in problems with your computer
- Data used on home computers may become infected with a virus, and contaminate your computer and other company computers

The list of potential problems goes on and on. Accordingly, get approval from management before making any changes to company computers.

Purchases of Computer Software and Equipment

Purchases of computer software and equipment are prohibited without approval from departmental management and information systems management. All computer software and hardware purchases must be registered with the information systems department, meet pre-established quality requirements, and be compatible with other company computer software and equipment.

Disposal of Company Data

Purge files that no longer have a practical use on a periodic basis. Old computer files utilize disk space, and often represent a potential hazard to you and the company. Delete old personnel evaluations, compensation information, sales and financial information, customer information, and vendor data. Typically, dated information is only useful to individuals who should not have the data.

A word of caution, permanently removing a file from your computer is something you need to consider carefully before taking action. Recreating a file you did not intend

to delete is tedious, and time consuming. Although the file probably exists on back-up, it is not always practical for the Information Systems Manager to expend the resources necessary to find the file. The LAN backup is principally designed to recover the entire system, not a single file.

File Recovery

Computer files and e-mail are rarely erased from the system simply by hitting the delete key. Rather, they are stored in a random place on the computer. These files can be easily recovered by running a file recovery program. To actually erase a deleted file from existence, you must run a program to erase deleted files. Keep in mind that if the files are backed-up before you run the program, you again have an electronic record. Files stored on the LAN are much more difficult to erase. This is because the LAN is backed up automatically, and only the Information Systems Manager has access to run programs that will permanently erase a file from the server. The bottom line is, your deleted file is most likely permanently stored on back-up.

Personal Use of Computers

Incidental and occasional personal use of company computers is permitted for reasonable activities that do not need substantial computer hard disk space, or other computer equipment. As a general rule, if you would be uncomfortable asking for permission, it is probably not an appropriate use of company computers. Prohibited activities include, but are not limited to, computer games, personal software and hardware, writing your autobiography, and running a personal business on the side. Using company computers to store or transmit inappropriate jokes, junk mail, chain letters, or to solicit for commercial, religious, charitable, or political causes is prohibited. If you are uncertain about a specific activity, ask your supervisor. Personal files, information, and use of company computers will be treated no differently by the company than business use, with regard to employee privacy.

Many software games are illegally copied, and often contain viruses. Such programs represent a potential liability to you and the company. Proof of ownership and management authorization for use is required for all software on company computers. Coming to work with a computer game, on an unlabeled disk, you received from a friend of a friend, who obtained it at a “Hacker’s Rule” convention, that may be contaminated with a virus that could corrupt other company computers, is prohibited. Proceeding to play the game on company time is irresponsible. We do not think in these terms when using computer games. However, it’s time we start.

Proprietary Information

Company data, databases, programs, and other proprietary information represent company assets and can only be used for authorized company business. Use of company assets for personal gain or benefit is prohibited. Sharing company proprietary information with company personnel, or third parties, is prohibited.

Reporting Policy Violations

Employees are required to report violations, or suspected violations, of computer policy. Activities that should immediately be reported to management include, but are not limited to:

- Attempts to circumvent established computer security systems
- Use, or suspected use, of virus, trojan horse, or hacker programs
- Obtaining, or trying to obtain, another user's password
- Using the computer to make harassing or defamatory comments, or to in any way create a hostile work environment
- Using the computer to communicate inappropriate messages or jokes that may be considered offensive by others
- Illegal activity of any kind
- Trying to damage the company, or an employee of the company, in any way

Computer policy violations will be investigated. Noncompliance with the company's employee computer policy may result in discipline up to, and including, termination. Employees that report violations, or suspected violations of company policy will be protected from termination, discrimination, harassment, and any other form of retaliation. Hackers, snoopers, password stealers, virus installers, data erasers, and anyone involved in such activity will be disciplined.

If you identify computer security vulnerability, you are required to report it immediately.

Termination of Employment

All information on user computers is considered company property. Deleting, altering, or sharing confidential, proprietary, or any other information upon termination requires management authorization. The computer you have been entrusted with must be returned with your password, identification code, and any other appropriate information necessary for the company to continue using the computer, and information, uninterrupted.

The following activity is prohibited upon termination, and will be prosecuted to the fullest extent of the law:

- Accessing company computers
- Providing third parties, or anyone else, access to company computers
- Taking computer files, data, programs, or computer equipment

Privacy

Monitoring Computer Communications and Systems

Many people think data stored on computers, transmission of data between individuals on dial-up modem lines, communications on the Internet, and e-mail are private, and in most cases they are. However, the company reserves the right, without prior notice, to access, disclose, use, or remove both business and personal computer communications and information, and will do so for legitimate business purposes.

Random audits to verify that company computers are clear of viruses, and used in accordance with company policy, may be performed. The company will investigate complaints about inappropriate images on computers, inappropriate e-mail, or other inappropriate conduct. The company may monitor Internet activity to see what sites are frequented, duration of time spent, files downloaded, and information exchanged. Again, computer systems and information are company property, and should be used principally for business purposes.

It is not the management's intention to be "Big Brother." However, it is management's fiduciary responsibility to:

- Establish and enforce policy to help prevent the violation of personal rights and illegal acts
- Reduce the risk of liability and business interruption to the company
- Maintain a professional work environment where computer abuse will not be tolerated

Lawsuits and Subpoenas

Company computers, like any other company property, are subject to subpoenas. This means that prosecutors and plaintiffs' attorneys may access company computers, and look at information to gather evidence in a complaint. It is not difficult to imagine how easy it would be to find embarrassing and possibly

incriminating information on company computers. For attorneys skilled in electronic discovery, the wealth of information is immense.

It is not management's intention to suggest that you remove any information from your computer, now or at any other time, to in any way hinder an investigation of any kind. Quite the contrary, management prohibits such activity. Management's intention is to ensure that users conduct their work to the highest ethical standard with the knowledge that computer information (even deleted files) can be used against you and the company in a legal proceeding.

External Communications

Third Parties

The same standards of decorum, respect, and professionalism that guide us in the office environment, apply to computer communications with third parties. Important, confidential, and proprietary information is stored on company computer systems. Accordingly, only company personnel are allowed access to the company's computer systems, without written authorization from management. Management must approve computer data and other information received by, or provided to, third parties. Please keep in mind that third parties may have a legitimate business need, duty, legal right, or obligation to access, disclose, or use information transmitted.

Dangers of the Internet

Ed Felten's Java-security team at Princeton University published an analysis of many ways that attackers can hijack information being sent to legitimate web sites by users; one example is to insert unauthorized hot links in a poorly secured web site.

An unauthorized hot link is a program installed on a legitimate web site by an unauthorized individual. The program changes, or adds to, the path of information transmitted. As such, the user may unknowingly send information to a location not authorized by the web site administrator, as well as the intended destination.

Copyright laws can be enforced on the Internet. Viruses can be downloaded from the Internet. Inappropriate web sites, images, and communications exist on the Internet. Competitors exist on the Internet. Hackers exist on the Internet. As such, users must follow established computer operating policies and practices to reduce the opportunity for security breaches, and inappropriate or illegal activity resulting from connecting to the Internet.

Internet Connections

Internet connections are authorized for specific business needs only. Connection to the Internet without management authorization is prohibited. Furthermore, the following activities are prohibited without management authorization:

- Accessing the Internet without an approved firewall
- Downloading information of any kind, including data, files, programs, pictures, screen savers, and attachments
- Exploring the Internet for fun or profit
- Establishing communications with third parties
- Research for personal or business purposes
- Forwarding or transmitting information to third parties or employees
- Copying programs, files, and data
- Transmitting important, confidential, or proprietary information
- Speaking on behalf of the company

Individuals that have received management approval to transmit information on the Internet should understand that such transmissions are identifiable and attributable to the company. Disclaimers such as "***The opinions expressed do not necessarily represent those of the company,***" while a good idea, do not necessarily relieve the company of liability. The Internet should be considered a public forum for all transmissions. All communications on the Internet provide an opportunity for a permanent record, and can be edited and retransmitted. Accordingly, maintain a professional decorum in all communications and transmissions.

The following actions are prohibited under any circumstances:

- Portraying yourself as someone other than who you are, or the company you represent
- Accessing inappropriate web sites, data, pictures, jokes, files, and games
- Inappropriate chatting, e-mail, monitoring, or viewing
- Harassing, discriminating, or in any way making defamatory comments
- Transmitting junk mail, chain letters, or soliciting for commercial, religious, charitable, or political causes
- Gambling or any other activity that is illegal, violates company policy, or is contrary to the company's interests

Business Reputations

Please keep in mind, a statement or posting of information on the Internet can cause serious damage, because information can be quickly and effectively

disseminated. The company, and the law, can and will hold you responsible for offensive, discriminatory, and defamatory statements, or any other illegal activity.

Remote Access

Users are required to turn off dial-up modems at the end of the day. Modems must be programmed to pick-up after the fourth ring (this will help prevent unauthorized access). Users are required to turn off remote access programs within a reasonable time after use, usually 5 to 10 minutes. Downloading or uploading confidential or proprietary information requires approval by departmental management and information systems management.

E-mail

Electronic Communications

E-mail is a wonderful tool. Used correctly, it can provide significant efficiencies, and improve the quality of the way we do business. It makes dissemination of information easy and cost-effective. Please take full advantage of it.

The same standards of decorum, respect, and professionalism that guide us in our face-to-face interactions apply to the use of e-mail.

Incidental or occasional use of e-mail for personal reasons is permitted. However, only company personnel are allowed access to the company e-mail system. The following e-mail activity is prohibited:

- Accessing, or trying to access, another user's e-mail account
- Obtaining, or distributing, another user's e-mail account
- Using e-mail to harass, discriminate, or make defamatory comments
- Using e-mail to make off-color jokes, or send inappropriate e-mail to third parties
- Transmitting company records within, or outside, the company without authorization
- Transmitting junk mail, chain letters, or soliciting for commercial, religious, charitable, or political causes

Employees are required to report inappropriate use of e-mail.

Dangers and Pitfalls of E-mail

Several large corporations including Citibank and Morgan Stanley & Co. have been sued for millions of dollars during the past year for contents of e-mail messages. Andersen Consulting is defending a $100 million lawsuit in which e-mail messages left on clients' computers by Andersen's consultants are expected to be key. COMPUTERWORLD magazine, September 8, 1997.

Appropriate e-mail etiquette is essential to maintaining a productive and professional work environment. Comments that might be made at parties, in elevators, and on the telephone are now done via e-mail. However, e-mail does not disappear into thin air. It can be widely, easily, and quickly disseminated. E-mail can be edited, forwarded, distributed, and filed for later use, possibly at the most inopportune time. For professionals with electronic recovery skills, e-mail is a gold mine. If you would not put it in a memorandum on company letterhead, do not say it with e-mail!

Rules of E-mail

Mark Grossman, author of Computer Law Tip of the Week and columnist for the South Florida Daily Business Review, believes in four basic rules for using e-mail:

- *Never, ever give bad news by e-mail. Bad news always deserves a real human voice, whether over the phone or in person*
- *Never use e-mail to criticize people. It stings much more in writing and does not heal with time. All day long, the recipient gets to reopen the e-mail and feel bad all over again. Critical e-mail inevitably eats at the craw of the recipient*
- *Never discuss personal issues over the office e-mail system. It's truly bad office etiquette. CC's being what they are, you may just see that personal e-mail posted on the lunchroom bulletin board. (Hint: Any e-mail that starts with "Oh, honey" is probably a personal e-mail that should not be in the office computer system.)*
- *If there is even the slightest possibility that what you are going to say could be taken wrong, don't use e-mail to say it*

Follow Mr. Grossman's four basic rules of e-mail. Keep in mind, e-mail is not the only form of communication (although at times it may seem that way). If you have something confidential or sensitive to say, there are better ways to communicate your message. It is still good practice to use the phone, or stop by someone's office and talk face-to-face. It worked for years before e-mail, and in many ways it works even better today.

Forwarding Information

E-mail makes attaching files and forwarding data a snap. However, the damage from forwarding something to the wrong person may be serious. Please take a minute to think through the appropriateness of all the parties you are forwarding. If you receive an e-mail (particularly e-mail with an attachment) and intend to forward it to others, consider the following:

- Is any of the information unnecessary or inappropriate for any individual?
- Would the author take exception to, or be embarrassed by, your forwarding the information? (A good rule of thumb is to copy the author.)
- Might the information be received negatively?
- Might the information be misunderstood?
- Is the receiver likely to forward the information to individuals that should not have, or do not need, the information?
- Do the attachments have viruses?

If the answer to any of these questions is yes, do not forward the information. Edit it, or create a new file. A bad decision only result in misunderstanding, hurt feelings, and added work.

Spam

Sending unsolicited messages or files to individuals, groups or organizations that you do not have a prior relationship with is prohibited, without written authorization from your supervisor. Sending messages or files with the intent to cause harm or damage to the intended receiver is a violation of company policy and will be prosecuted to the full extent of the law.

Intranet

The company Intranet, like e-mail, is a wonderful tool. It can provide significant efficiencies; and it makes dissemination of information easy and cost-effective.

Data, programs, and other information are updated regularly on the Intranet. As such, it is your responsibility to ascertain that information you are working with is current.

The same standards of decorum, respect, and professionalism that guide us in the office environment apply to the use of the Intranet. Important, confidential, and proprietary information is stored on the Intranet. Accordingly, only company personnel are allowed access to the Intranet, without written authorization from management. All company policies apply to use of the Intranet. The following activities are prohibited, without management authorization:

- Installation of a web site, page, or any other information
- Installation of business or personal software on the Intranet
- Exceeding authorized access of Intranet programs, data, and files
- Assisting anyone outside the company in obtaining access to the Intranet
- Making any changes to the Intranet hardware or software

Local Area Network

All important, confidential, or proprietary information must be stored on the LAN. Storing information on your desktop computer is prohibited, without authorization from management. The LAN is equipped with electronic and physical security. Activity on the network is monitored for tampering and other security breaches. Maintenance and back-up are performed on the LAN daily; and programs and other information are updated regularly. Use the LAN! It is safe, effective, and reliable. Because important, confidential, and proprietary information is stored on the LAN, only company employees are allowed access, without written authorization from management. All company policies apply to the LAN. The following activities are prohibited, without management authorization:

- Installation of business or personal software on the LAN
- Making any changes to the LAN hardware or software
- Accessing without authorization, or exceeding authorization, LAN programs, data, and files
- Assisting anyone within, or outside, the company in obtaining access to the LAN

Receipt of
Employee Computer Operating
and Security Policy

I have received and read the company's Employee Computer Operating and Security Policy. I understand that I am responsible for adhering to the policies and practices described therein. I understand that these policies may be added to, or changed by the company at any time. It is my responsibility to bring any questions I have about the Employee Computer Operating and Security Policy to my supervisor. I further understand that it is my responsibility to report any violations of this policy that I witness, or become aware of, during the course of my employment.

_____ _____

Employee Signature Date

_____

Employee Name (Please Print)

Glossary of Terms

Computer Information
Data, software, files, and any other information stored on company computers and systems.

Encryption
The process of turning plain text into cipher text by applying an algorithm that rearranges or changes its input into something unrecognizable.

Firewall
A specifically configured system that serves as a secure gateway between an outside network (e.g., the Internet), and the organization's internal networks.

Hacker
Slang, an individual intensely absorbed with and/or extremely knowledgeable about computer hardware and software. Also used to describe those who break into and corrupt computer systems. (Hacker is used here to describe those who break into and corrupt computer systems.)

Hot Links
A connection made between application programs so that when changes are made to the data in one file, the changes appear instantly in another.

Intranet
A local area network which may not be connected to the Internet, but which has some similar functions. Some organizations set up World Wide Web servers on their own internal networks so employees have access to the organization's Web documents.

Internet
The mother of all networks. A group of networks connected via routers.

ISDN
Integrated Services Digital Network. Digital telecommunications lines that can transmit both voice and digital network services, and are much faster than the highest speed modems.

LAN

A set of connections between computers that provides the basis for electrical transmissions of information, generally within a small geographical location to serve a single organization.

Login

A start-up file stored in the user's directory. This file is used to execute commands that should only be executed at login time, such as establishing the terminal type and starting windows systems.

Modem

Short for modulator-demodulator. A hardware device that allows two computers to communicate over ordinary telephone lines.

RAM

Random Access Memory. The working memory of the computer. RAM is the memory used for storing data temporarily while working on it, running applications programs, etc. "Random Access" refers to the fact that any area of RAM can be accessed directly and immediately.

Server

A computer or device that administers network functions and applications.

Trojan horse

A program that masquerades as something it is not, usually for the purpose of breaking into an account or exceeding commands with another user's privileges.

Virus

A set of instructions that can reside in software; and can be used to destroy other files or perform other tasks with another user's privileges.

Web Site

A server computer that makes documents available on the World Wide Web. Each web site is identified by a host name.

Worm

A program that propagates by replicating itself on each host in a network, with the purpose of breaking into systems.

Computer Misuse Organizations are Experiencing

If employees are expected to meet company expectations with respect to computer privileges, they need comprehensive computer policy. Without computer policy in place, management can expect computer abuses like the following to continue, and the company may ultimately be held liable.

Internet —The Great Playhouse

*A survey by A.C. Nielsen found that in **one month**, employees at IBM, Apple, and AT&T spent the equivalent of **1,631 workdays** (13,048 hours) on the site of Penthouse Magazine*

Compaq computer fired more than a dozen workers in Houston last year after they registered more than 1,000 visits to sex sites from work. San Diego Union-Tribune, August 1997.

PC World magazine reports that one in five companies have disciplined employees for improper Internet use. More interesting, the magazine reports that only a third of the companies monitor Internet use.

Dangers of E-mail

When a mid-level executive at a West Coast company lost her job, her boss pointed to a tough economy. But what they didn't know is that buried deep inside the firm's computer system was an old derogatory e-mail message assumed to have been deleted long ago.

"Get the bitch out of here as fast as you can," said the message, from the woman's supervisor to another. "I don't care what it takes."

Hours after computer sleuth John Jessen unearthed it, the firm wrote the woman a check for $250,000 to settle her lawsuit. Chicago Tribune

*In 1995, Chevron Corporation paid more than $2 million to four female employees to settle their claim that they were harassed by sexually explicit **e-mail** messages, including **"25 reasons beer is better than women."** COMPUTERWORLD Magazine*

Computer Sabotage — It Happens

Authorized computer users, predominantly employees, commit most inappropriate, negligent, and unethical computer activity. Security experts estimate that at least **75 percent** of computer sabotage comes from inside the company, not from outside hackers. According to a survey sponsored by the American Society of Chartered Life Underwriters and Chartered Financial Consultants and the Ethics Officer Association ***45 percent*** *of workers say they committed one of a dozen actions over the past year that were either* ***unethical, or fall into a gray area.***

At General Dynamics Space Division in San Diego, a programmer, unhappy with the size of his paycheck, planted a software program — known as a "logic bomb" — designed to wipe out a program to track Atlas missile parts. Fortunately, during a routine check of programs stored on the system, a fellow programmer discovered the logic bomb and removed it before it was activated. Underground Guide to Computer Security

Omega Engineering in Bridgeport suffered $10 million in productivity losses after someone unleashed a "logic bomb" in their computer system. USA Today

Computer Crimes

Who is committing computer crimes? According to the Underground Guide to Computer Security, it is current and former employees that commit most computer crimes. Computer Science Corporation echoes this position in EDUPAGE, A Summary of News about Information Technology, when the company warned that many organizations are being attacked by ex-employees or by ex-employees of outsource computing services.

Federal sentencing guidelines provide substantially higher fines for organizations:

- ***That do not have in-house programs*** *to prevent and detect violations of the law*
- *Where an individual in a high-level position participated in****, condoned, or was willfully ignorant*** *of the offense*
- ***Where tolerance of the offense*** *by individuals with substantial authority* ***was pervasive throughout the organization***

The Mentality of the Digital Age

Don Pavlish created the web site "Don's Boss Page" that features tips and tricks on how to look busy while you are surfing the web. Don admits to browsing his favorite online magazines as a way of unwinding on the job, he sees the issue as a matter of workers' rights in the digital age. New York Times

The Security Fallacy

The CEO sat quietly as I showed him the complete manufacturing instructions for his top product in development. He remained expressionless when I placed his company's master development schedule on his desk. He leaned back in his chair as I pulled out several documents describing his bargaining position in a multimillion-dollar lawsuit.

The CEO finally spoke. "I guess we should be happy you're not working for a competitor."

I had stolen all of this and more posing as a temporary worker after the security manager called upon me to test just how much a dedicated information thief could get. I was there for three days. I got everything they had. SC InfoSecurity News Magazine

Although issues like the one above are typically considered more of an information systems security issue, than a computer user issue, the solution is complex. Much of the information the "dedicated information thief" got would not have been obtained except for employees and management sharing confidential information about the company's computer systems and information.

When we think of computer security we think of passwords, hackers, viruses, earthquakes, etc. Levi Strauss' sensitive data was the victim of a screwdriver. A hard disk containing the names, birth dates and Social Security numbers of thousands of employees was stolen from the apparel maker's San Francisco headquarters. Company officials had to warn 20,000 of their U.S. employees that their personal data may be in the hands of thieves. The stolen information could be used to apply for a fraudulent credit card in the employee's name or gain access to other information about the employee. And the stolen hard disk contained bank account numbers for retired workers who opted for direct-deposit pension checks. COMPUTERWORLD magazine

Big Penalties for Copyright Infringement

Software is protected by the Copyright Act, and the Copyright Protection Bill. **Penalties include up to $250,000 and 5 years in prison, per incident.** The Copyright Software Rental Amendments Act of 1990 states that it is illegal to rent, lease, or lend copyright software without the authorization of the copyright holder.

The Software Publishers Association (SPA), one of the largest and most influential software industry watchdog associations, encourages employees, former employees, temporary employees, and consultants to inform on companies suspected of using illegal software. The SPA provides an 800-hotline number for informants, and often gets up to 800 calls per week to the hotline. The SPA has, and will get the FBI and local authorities involved if copyright infringement is suspected.

The following is just one example of the many copyright infringement cases reported in the SPA's online newsletter. It began with a simple telephone call (from an informant) to the SPA's 800-hotline number:

A Florida-based private junior college, International Fine Arts College, Inc., paid $135,000 to settle a lawsuit alleging copyright infringement. The complaint alleged that International Fine Arts College had unlawfully duplicated computer programs published by Adobe Systems Inc., Novell Inc., and Quark Inc. The court issued an ex-parte temporary restraining order one week later, which allowed the plaintiffs' representatives, accompanied by deputy United States marshals, to audit the computer programs installed on the defendant's computers.

Edward Porter, president of the college, stated ***he had no knowledge of the practices alleged and has issued a firm policy warning the college's employees about the importance of complying with copyright laws.*** *"The college is today in complete and full compliance with all copyright laws," Porter said.*

Computer Monitoring — A Privacy Issue

Currently, there is a legal issue as to whether certain information on company computers is private. Federal law does not establish a general right to privacy in the workplace. However, some states, including California, provide an employee a legal right to privacy. At this point, case law appears to favor the company when employees' rights to privacy in the workplace are litigated. However, if the company intends to monitor, in any way, employees' use of computers, in most situations it is best to disclose it to the employees. (Studies show that companies that disclose to employees that they monitor computer activity see a substantial decline in computer misuse.) Disclosure to users will minimize any legal exposure the company has under privacy laws, reduce the occurrence of computer abuse, and help uphold management's integrity with employees by being above board. Furthermore, telling

employees the reason why the company monitors computer activity helps users understand the policy's intent.

Who's Liable When Computer Abuse Occurs? — Maybe You!

Who is liable when computer abuse occurs? It depends upon the circumstances of the case. However, juries often have a funny way of determining who is liable when the plaintiff is a former employee who has provided years of dedicated service, received numerous above average personnel evaluations and merit increases, and was never provided with policy or trained on the proper use of company computers.

Appendix

Who You Can Contact if Your Computer System is Hacked Into

If management suspects a computer security violation and does not know what to do, contact the **CERT Coordination Center (CERT/CC) at Carnegie-Mellon University** at www.cert.org. For emergencies outside regular business hours, phone 412-268-7090. CERT/CC is a nonprofit organization established to help detect and prevent computer security breaches. CERT/CC policy is to keep information specific to your site confidential, unless they receive your permission to release the information

Special permission to reference the CERT® Coordination Center in ***Employee Computer Policies Made Easy*** is granted by the Software Engineering Institute.

Readers may learn more about CERT® Coordination Center on the Internet at http://www.cert.org.

CERT® registered in the U.S. Patent and Trademark Office.

Employee Termination Computer Checklist

Require all terminating employees to complete a "Computer Termination Checklist." When employees leave the company they are often required to turn in keys, credit cards, sign termination forms and complete other requirements of the human resources termination checklist. However, it is rare that the human resources department has an employee termination computer checklist. When employees are terminated, the process should include completing a questionnaire similar to the following:

I. Do you have a laptop, desktop or other computer equipment? (It is surprising how many employees leave with a company computer.)
II. Do you have any disks with important, proprietary, confidential or sensitive information on them?
III. Do you currently have access to company computers? If so, which ones?
IV. Has your user identification code and password been canceled?
V. Did you delete or substantially alter any computer data, files or programs upon your termination?
VI. Is there any reason that the company cannot access, or will have difficulty accessing, computer information previously controlled by you?

VII. Lastly, require a terminated employee to sign a statement that they not try to gain access to any of the company's computer systems or provide information to help others gain access to company computer systems

Computer Disclosure Statements

Consider presenting the following messages periodically on user computers.

No Trespassing Compliance Statement

Unauthorized access of company computers is prohibited. Any form of tampering, including snooping and hacking, to gain access to company computers is a violation of company policy and may be subject to civil and criminal prosecution. (This message should always appear when anyone is using remote access software to access company computer systems.)

E-mail Disclosure Statements

The information transmitted is intended only for the person or entity to which it is addressed, and may contain confidential and privileged information. Any review, retransmission, dissemination, or other uses of this information by persons or entities other than the intended recipient is prohibited. If you receive this in error, please contact the sender and delete the material from your computer.

E-mail may be altered electronically, the integrity of this communication cannot be guaranteed.