



Texas Wesleyan University Information & Communication Technology Information Security Policy

This document describes the Information Security Policy for Texas Wesleyan University (TW). It describes procedures for protecting Software and Computer-Based Information (SCBI).

All employees of TW have an ethical and moral obligation to protect proprietary information owned by or under the custody of TW, and to maintain the confidentiality of this proprietary information. This policy is meant to provide the requirements for necessary and appropriate controls, while providing an environment in which employees have access to all required information and an enhanced ability to perform their jobs functions and responsibilities through a better understanding of the framework within their jobs and responsibilities should be carried out.

CONTEXT

All the procedures apply to the TW facilities, communication facilities including access to the TW network either inside the University or through the connections to other networks or Internet, and information.

Any TW site using subcontractors for some or part of its Information Technology operations (for instance, facilities management or records storage) must contractually impose the same or equivalent security rules on the subcontractor.

DEFINITIONS

Security enclave: It is a contiguous part of a network that is under a common security policy.

Security domain: It is a set of security enclaves under a common authority jurisdiction.

User Groups: Users accessing information or services from one of the Security enclaves. These users can be lumped together themselves part of a security enclave/domain or can be dispersed across a network.

Threat: Is the danger level an information asset is exposed to via network resources.

Risk: Is the probability that an attack will occur on an information asset based on the associated threats and its value.

Security Officer: Person responsible for the administration and application of the security procedures and recommendations stated in this policy.

AUTHORITY

The Vice-President (VP) and/or Chief Information Officer for the locations are responsible for implementing this policy. The Site Security Officer ("Security Officer") is responsible for the administration and application of this policy and the security procedures. The Security Officer will report security incidents to the appropriate VP or CIO. All personnel who have access to secure computer rooms and/or SCBI, and all users of those computers and SCBI, are responsible for upholding this policy and reporting any violations to the Security Officer.

The Security Officer can, in agreement with the appropriate VP or CIO, add a new statement not considered before in this document, in order to cover unusual situations that may arise in the future.

DISTRIBUTION

Periodically, there will be general meetings to discuss security. The Security Officer will make the security policy available for anyone to review. Each employee will be briefed on security at least once per year.

This policy shall be made available to new employees when they are hired, and it also shall be accessible for all the existing personnel after every review or modification.

The Security Officer shall require new employees and long-term visitors, as well as existing employees, to formally acknowledge that they have read this security policy and sign an agreement of acceptance of this policy. The Security Officer may also recommend disciplinary action for any employee who deliberately or repeatedly violates security policies.

REVIEW

This policy is effective immediately. Any modifications to this policy must be approved by the Vice President of Finance and Administration and Provost and/or Chief Information Officer. Each January, the Security Officer must review the policy to ensure that it is relevant to University needs, corporate policies, and that it reflects current technology. The Security Officer will conduct this review and make appropriate recommendations to the Vice Presidents and Chief Information Officer for modifications.

RISK ANALYSIS

This section outlines the assets that must be protected, and from what threats; since the loss of an asset represents a significant loss to the University. In some cases, a lost asset cannot be replaced, particularly in the case of goodwill, trust, or confidential research. This is necessary to provide the underlying logic for the following sections which formally define the rules that apply to the use of those assets.

The principal assets to be protected are: data and information, documentation, goodwill and reputation, hardware, people and skills, and software.

The loss of an asset is caused by the realization of a threat. The threat is realized via the medium of vulnerability. Threats cannot be controlled within a University as a threat is essentially a product of the University's environment. This is not so for vulnerabilities, which usually exist within the University. Hence the purpose of the security policy and its associated procedures is to minimize the number and size of any vulnerabilities and thus negate any potential threat and its impact on a University's assets should a threat be realized. Examples of threats that may be examined are:

Denial of Service (DOS)

Computers and networks provide valuable services to their users. Many people rely on these services in order to perform their jobs efficiently. When these services are not available, a loss in productivity results.

Denial of service comes in many forms and might affect users in a variety of ways. A network may be rendered unusable by a rogue packet, jamming, or by a disabled network component. A virus might slow down or cripple a computer system. Each site should determine which services are essential, and for each of these services, determine the effect to the site if that service were to become disabled.

Destruction (of assets)

The information, as well as other resources, should always be available to the users. One common threat consists in the destruction of the physical resources and the deletion of the stored information. Each site must determine the cost associated with the continuous replacement of the erased information, and consider the costs of protecting these assets against this kind of threat.

Disclosure of Information

Another common threat is disclosure of information. Determine the value or sensitivity of the information stored on your computers. Disclosure of a password file might allow for future unauthorized accesses. A glimpse of a project may give a competitor an unfair advantage. A technical paper may contain years of valuable research.

Theft (of information or physical assets)

This threat is very similar to the destruction of physical assets in a sense that they have the same effect to the University. In the particular case of theft of information, the risk is even higher since the University's classified information may be very valuable to the competitors.

Unauthorized Access

A common threat that concerns many sites is unauthorized access to computing facilities. Unauthorized access takes many forms. One means of unauthorized access is the use of another user's account to gain access to a system. The use of any computer resource without prior permission may be considered unauthorized access to computing facilities. Through unauthorized access, an intruder can make other attacks such as theft, disclosure or destruction of information, or denial of service.

SECURITY RULES

This section defines the rights and responsibilities of users and the resource provider in order to preserve the security of the assets defined hereby. This section has been divided in different subsections for the sake of clarity.

USER SECURITY

HIRING POLICY

The Human Resources Department (HR) shall orient new employee, consultants, contractors, and temporary employees who will have access to communications and computing services to the contents of this policy. They should emphasize the privacy of users' electronic mail, files, and data. HR will obtain a signed copy of the security policy cover page from the new employee and add it to the employee's personnel file. Specific detailed questions about this policy can be directed to the Security Officer for further clarification.

TERMINATION/TRANSFER POLICY

Terminated users will be denied access to systems. HR must immediately notify the Security Officer or his/her designee whenever a user's status changes; and this notification should be recorded in the Human Resources Department's Termination Checklist. Status changes include, but are not restricted to, terminations, transfers, and leaves of absence. Upon termination, access to personal information maintained on systems may be denied.

When a user leaves the University, the user account and electronic mailbox shall be closed. However, if the user is transferred to a different campus thus prompting the need for a new e-mail alias, the employee may request the account with the old e-mail alias remain active for 30 days. It is the responsibility of the employee to move all needed e-mail files from the old mailbox to the new mailbox before access is terminated. Electronic mail shall not be automatically forwarded outside of the University's network.

ACCOUNT REQUESTS

All new and current TW employees should complete and submit the Account Authorization Request form to the ICT Help Desk to gain access to the campus network and TW e-mail services.

Shared drive and shared e-mail accounts are available to academic and administrative departments. Interested departments should complete and submit the Shared Account Request form.

Current TW employees are eligible to sponsor a temporary account for persons not affiliated with TW (such as external program students, consultants, or temporary workers). The account sponsor should complete and submit the Sponsored Account Request form. These persons will be subject to all TW information technology policies and the account sponsor will be accountable for the actions of those under his/her supervision.

ACCOUNT SECURITY

USER ACCOUNTS

User accounts shall only be assigned to current employees and students, sponsored non-employees requiring temporary access to the network resources, and sponsored third parties who have executed the proper non-disclosure and patent agreements.

Sponsored accounts shall be granted for seven days duration, unless the conditions of access are covered by an explicit written agreement with the party in question. They can be renewed upon request by the current eligible employees.

All the accounts are strictly for individual use. Users shall not let anyone use their account under any circumstances, so only authorized people may have access to the network resources. Users shall not disclosure login and/or password information under any circumstances.

All user accounts must have password protection. Password security must be maintained at all times. Anonymous accounts, group accounts, and shared passwords are strongly discouraged and may only be authorized by the Security Officer. Additional protection and restrictions will be necessary to access privileged accounts. All users are responsible for managing their accounts and passwords. Users should choose a secure password for his/her account. A sample set of guidelines for password selection is shown below:

DON'TS

- DON'T use your login name, first, middle, or last name in any form (as-is, reversed, capitalized, doubled, etc.).
- DON'T use your spouse's or child's name or other information easily obtained about you. This includes expressions peculiar to one's profession, words listed in standard available reference materials, license plate numbers, telephone numbers, social security numbers, the make of your automobile, the name of the street you live on, etc.
- DON'T use a password of all digits, or all the same letter.
- DON'T use a word contained in English or foreign language dictionaries, spelling lists, or other lists of words.
- DON'T reuse Passwords once they have been expired or changed.
- DON'T use a password shorter than six characters. Passwords should be at least eight characters long.
- DON'T store non-encrypted passwords on the system.

DOS

- DO use a password with mixed-case alphabetic characters.
- DO use a password with non-alphabetic characters (digits or punctuation).
- DO use a password that is easy to remember, so you don't have to write it down.
- DO use a password that you can type quickly, without having to look at the keyboard.

Methods of selecting a password which adheres to these guidelines include:

- Choose a line or two from a song or poem, and use the first letter of each word.
- Alternate between one consonant and one or two vowels, up to seven or eight characters. This provides nonsense words which are usually pronounceable, and thus easily remembered.
- Choose two short words and concatenate them together with a punctuation character between them.

Users should also change their password periodically, usually every other month. This makes sure that an intruder who has guessed a password will eventually lose access, as well as invalidating any list of passwords he/she may have obtained. If the Security Officer believes that a user password might be in use by a non-authorized person(s), he can notify the user of this situation and request s/he change the password immediately.

If a user forgets his/her password, a new password must be assigned. The owner of the account must request this change in person showing either their TW Photo ID Card or a State Issued ID Card or Driver's License

If a system is compromised by an intruder, all passwords on the system must be changed. Users will be notified of such actions with a message telling them that they should change their password(s) immediately. If the password isn't changed before the time period expires, the account will be locked and can be opened by contacting the Help Desk and providing the representative with your TW Employee/Student ID number.

This e-mail message will not include a request to change the password to a specific one. If a user receives a message asked to change the password to a specific one, they must communicate this event to the Security Officer (ext. 4428) and ignore the message.

Users should not leave interactive sessions logged into their accounts when they are not at the computer. In any event, users should lock their office when they leave for an extended period of time.

Every personal computer must be secured with a "POWER ON" internal password and a "SCREEN SAVER" password.

PRIVILEGED ACCOUNTS

The following procedures shall be used to manage privileged accounts:

- Generally, only TW authorized staff may have accounts with UNIX "root" or PC "administrator" privileges. Requests for similar access by other personnel must be approved by the Security Officer.
- Only key personnel who are directly involved with management or administration of a computer may be granted access to an account with non-standard privileges.
- In all cases, privileged users will respect the privacy of an individual's electronic mail, data files, and information. They shall obtain the individual's approval to access the private information or use special problem analysis tools, unless otherwise directed by the user's immediate supervisor or Security Officer.

- Privileged users shall not leave computer consoles or workstations unattended if they are logged into a privileged account. However, privileged users may utilize password-protected "screen saver" programs.
- Privileged users may disclose account passwords only on a "need-to-know" basis. The passwords should be changed as soon as possible thereafter.
- Privileged users shall not write account passwords on paper or other media.
- Privileged users shall also have a non-privileged account in which they should perform as much of their work as possible.
- Privileged users shall change their passwords more frequently, or have a longer password length than the standard user account. Acceptable password length and frequency of change shall be approved by the Security Officer.

Whenever a privileged user leaves the University or no longer has need of the privileged account, the passwords on all privileged accounts should be changed.

SPONSORED PROJECT ACCOUNTS

The following procedures shall be used to assign and access sponsored project accounts:

- If project security or software engineering practices so dictate, a separate project account may be established with approval of the Security Officer and sponsorship by a current TW employee.
- Each project account shall have its separate operating system "account group". Only those users who need to access the files stored under this account shall become members of that "account group".
- The default file protections for the project account shall be set up to restrict access to non-project members.
- Responsibility for the project account must be assumed by the TW employee sponsoring the account and customary practices for user or privileged user account management must be followed.

SPONSORED ACCOUNTS

The following procedures shall be used to access sponsored guest accounts:

- The TW LAN support staff, by proper request, shall provide and maintain a restricted guest account for use by visitors to the University for a short period of time (less than one week).
- The sponsored guest account shall provide only a limited subset of capabilities, principally so that visitors may access their personal accounts on remote systems.
- The sponsored guest account shall be set up to prevent access to SCBI on other accounts.

ACCOUNT INSTALLATION

Care must be taken when installing accounts on the system in order to make them secure. When installing a system from distribution media, the password file should be examined for "standard" accounts provided by the vendor. Many vendors provide accounts for use by system services or field service personnel. These accounts typically have either no password or one which is common knowledge. These accounts should be given new passwords if they are needed, or disabled or deleted from the system if they are not.

If the operating system provides a "shadow" password facility which stores passwords in a separate file accessible only to privileged users, this facility should be used.

All user accounts shall be audited quarterly for active status. All accounts that have been inactive for six months shall be disabled. In all cases, TW is not responsible for personal information maintained on the network systems.

ACCOUNT NAMING STANDARDS

Account names must be chosen to provide a unique identification for the user. If feasible, they should also be unique within the TW's network community. Users with accounts on multiple systems shall use the same account name on all systems. As a general guideline, the user's first initial and last name will form the account name. The middle initial of the user's name may be included to generate unique account names. Additional identifying numbers may be added as necessary.

In situations where account name conflicts are identified, both users must change their account names to avoid future conflicts, resolve confusion of which person did not change, and avoid the inevitable SCBI associated errors. Project accounts should attempt to incorporate the name of the group or project into the account name, instead of the user's name.

FILES AND DATA SECURITY

All the files and archives within the network are considered as Proprietary Information. Users shall not disclose any of this information without previous authorization.

Vendors and consultants may be given access to proprietary information only on a need-to-know basis, and in each case shall be required to sign a confidentiality agreement (the form of this agreement is the responsibility of the TW Legal Department). Non-TW information may be disclosed by TW to third parties only in accordance with the terms and conditions under which it was received.

In cases where non-employees who are not covered by a confidentiality agreement need to have access to proprietary information, computer system or network resources, the access shall only be allowed under the direct and continuous supervision of an authorized employee.

Electronic communications among TW personnel and/or third parties shall be treated with the same confidentiality as other, more traditional forms of communication (e.g., postal mail, telephone) as stated in the Electronic Communications Privacy Act. The contents of a communication usually dictate the degree of confidentiality required.

Electricity malfunction may permanently damage the machine or the data contained in it. It is strongly recommended, especially in those areas with continuous or random electricity instability, to have every personal computer protected with stabilizers.

Personal computers used to run sensitive data, such as the Financial Systems, should also be protected with adequate UPS's (Uninterrupted Power Supply) to ensure that no data is lost in the event of unexpected electrical power cuts. UPS's ensure an additional period of electricity which allows to terminate pending jobs in a controlled manner.

Sensitive data files should be protected by document passwords. Document passwords can be activated during the **Save As- Options** function and exist in systems such as Word, Power Point and Excel. It is strongly recommended that a unique document password be used by the same user for all documents secured with this method.

System users should be made aware that printed forms such as checks, invoices purchase orders and statistical reports in general, could be used to divert information to unauthorized users. Distribution or display of reports to unauthorized individuals could inadvertently create opportunities for information disclosure or defalcation. Sensitive reports could be used to TW disadvantage if they fell into the wrong hands. These risks are controlled through responsible users, good distribution and storage procedure, and finally destruction of sensitive outputs.

Users are encouraged to use proper etiquette and follow all applicable guidelines when sending electronic mail. Users may only use the e-mail system for official university communications. Users shall not send controversial mail or postings to mailing lists or discussion groups (obscenity, harassment, etc.) nor use offending language in the messages.

Unrestricted file access which would allow sensitive files to be copied across computer networks is prohibited. Users and product groups are responsible for maintaining the proper protections on sensitive files. File owners and product groups should periodically audit their files to insure compliance. Only TW computers can mount or access TW disks, unless the Security Officer provides prior authorization to do so.

When installing a system from the distribution media or when installing third-party software, it is important to check the installation carefully. Many installation procedures assume a "trusted" site, and hence will install files with world write permission enabled, or otherwise compromise the security of files.

Users shall not modify files that are not their own even if they happen to have write permission, unless they are authorized by the owner of the file.

LICENSED SOFTWARE

All software obtained from commercial vendors or "shareware" distributors that is used within TW must be appropriately licensed and paid for or otherwise legally obtained. Unauthorized copies and unlicensed use are explicitly prohibited. All software installations are to be completed by ICT following the appropriate software installation policy.

Unrestricted copying of software products for use on multiple machines is prohibited without the express written permission of the vendors or distributors involved, since is a violation of the copyright laws. To be considered "Compliant" all such agreements should be forwarded and kept on-file with ICT.

Copyrighted and licensed software may not be duplicated unless it is explicitly stated that you may do so. When in doubt, DON'T COPY.

TW-written computer program source code, program and equipment design documents, and listings shall be made available only to sites specifically authorized to develop software and equipment except for that normally required for maintenance activities. Program source media shall show author, site, date, copyright, and proprietary notice. The following is an approved notice:

© Copyright Texas Wesleyan University, unpublished work, created <date>. This computer program includes Confidential, Proprietary Information and is a Trade Secret of TW. All use, disclosure, and/or reproduction is prohibited unless authorized in writing by an officer of Texas Wesleyan University. All rights reserved.

Unrestricted file access which would allow sensitive files to be copied across computer networks is prohibited. Users and product groups are responsible for maintaining the proper protections on sensitive files. File owners and product groups should periodically audit their files to insure compliance.

Users shall not modify files that are not their own even if they happen to have write permission, unless they are authorized by the owner of the file. Users shall not access files stored under another student/employee account, unless they are authorized by the owner of the account.

UNIX FILE SECURITY PROCEDURES

Every individual and group is responsible for the proper level of security that is applied to files resident in their personal accounts, managed applications, or within the scope of their projects. In particular, it is paramount that the security and integrity of our customers and their SCBI is carefully maintained at all times.

User or system log-in procedures shall not have UNIX "OTHER" write access. Default file protection shall be set up to disallow OTHER access. File systems should be configured to disallow OTHER access to unauthorized users or groups. Use of ".rhosts" and ".forward" files on UNIX systems is discouraged, but they may be used with approval from the Security Officer when strong reasons justify doing so. All system startup files shall be owned by the "root" account. Single-user reboots shall require a password on non-secure workstation consoles.

All files required for the captive guest accounts shall be owned by the "root" account.

BACKUP STRATEGY

Shared Drive Backups

All files necessary for departmental operation shall be stored on the departmental shared drive and backed up on a regular basis. It is the responsibility of the department supervisor or his/her designee to stay within their allotment of disk space, ensure that all mission critical data is stored on the shared drive, and to archive older document versions.

That data on the shared drive will be regularly backed up by the ICT department as described in the *Server Backups* section of this document.

Server Backups

Full backups shall be performed at least once a quarter. Incremental backups are performed at daily (weekdays), weekly, and monthly levels. A full backup set shall be retained semi-annually at a secure off-site storage site for an indefinite period of time.

PC and Notebook Backups

Users are responsible for copies of their individual disks for all desktop and notebook systems.

Always maintain regularly scheduled backups of data as described below:

- Users should always back up critical data on the H: drive at least twice each year.

Restore Procedures

In the case of data loss, restore all files to the appropriate media as soon as practical limits will allow.

PHYSICAL SECURITY

Areas where personal computers and back ups are located must be secured by fire detection devices. Sprinkler systems might be a disadvantage because they can cause water damage to computer equipment and files.

Each office must keep an updated inventory of existing technology hardware items which should include asset tag number or serial number (items lacking an asset tag number), equipment type (computer, printer, monitor, etc.), and model name.

Each office must turn in an inventory of technology hardware items assigned to their personnel with the required information once per year (February).

Every movement of technology hardware items should be handled through ICT and a record of asset transfers should be properly handled.

Portable notebook computers, due to their small size, are extremely easy to steal. An adequate control must be kept over third parties or employee leaving TW facilities with equipment or bags, which might hide such portables.

All network access points must be allocated in secure areas. In cases where this requirement is not met (i.e. network access points in conference rooms), these points must be disabled and shall only be enabled when required and under the supervision of an authorized employee.

Only approved personnel should have access to computer rooms. All of these facilities should be locked during non-business hours.

Clients, vendors, consultants, and temporary employees may gain physical access to TW machines only when access is requisite to their successful completion of their duties, and in all cases, they must have an account sponsor and sign confidentially agreements when appropriate.

All computers, servers, and workstations shall display a log-in banner warning that access is limited to authorized personnel. Unauthorized personnel who attempt to use network facilities will be prosecuted to the fullest extent of the law when they are apprehended. Whenever possible, all server machines should be located in locked, environmentally-suitable rooms. These rooms must provide the necessary protection against unauthorized personnel, fire, water damage, electrical outages, etc.

If machines cannot be physically secure, care should be taken about trusting those machines. Sites should consider limiting access from non-secure machines to more secure machines. In particular, allowing trusted access (e.g., the BSD Unix remote commands such as rsh) from these kinds of hosts is particularly risky.

REMOVABLE MEDIA

When storing removable media, the following procedures shall be followed:

- Backup and archive tapes containing sensitive data or software shall be stored in secure areas with limited access, and they shall be effectively labeled as containing SCBI.
- A disaster protection scheme shall be devised for all backup and archive tapes vital to the operations.

The following procedures shall be followed concerning media for portable computers:

- TW SCBI stored on floppy disks is discouraged, but allowed for individual data. The preferred medium for storage of individual data is the USB Key (static state device).
- SCBI information stored on magnetic tape or optical disk shall be stored locally on a secure TW site, or under the direct personal management of a TW employee. It must also be effectively labeled to show it contains SCBI.
- SCBI information stored on magnetic disks or other media physically enclosed in portable computers must be network-protected with a password-oriented protection mechanism. It must also comply with the requirements for "File Security" as described in this policy.
- Access to the SCBI information on this media, or the repair of the media containing SCBI that is not reformatted, shall be supervised directly by a TW employee during the duration of access or repair.

NETWORK SECURITY

Under any circumstances legitimate users may attempt to break into other accounts, disrupt services or try to find other users passwords. This also applies to releasing worms, viruses, and other activities that may attempt against system security and/or performance such as network packet-reading software, etc. Administrators or groups who need to "hack" services for security research purposes shall address to the Security Officer for a proper authorization.

Special equipment with extremely sensitive data or destined to network research experiments shall be isolated from the TW network.

For detailed information related to network security, review the *Acceptable Use of Network Resources Policy* document.

REMOTE/WEB ACCESS

Access to the Internet is provided via WAN services from the TW Firewall. This service is provided for the transmission of electronic mail, access to network bulletin boards ("Usenet News"); access to "anonymous FTP", gopher, WAIS, and World Wide Web (WWW) sites; access to commercial vendor licensed software distributions and patches; and telnet (remote log-in) access from TW computers into the Internet only.

Off-site connections to some TW network resources is permitted using Web access tools (Homefile, WebAdvisor, WesNet, RamMail, etc.). Access requires a valid User ID and Password.

VIRUSES

The principle danger of importing files and software, whether over the LAN or installation from portable media, is virus infection. Thus, it is the responsibility of the end user who is performing the importation or installation of any software, files and data into the communications and computing domain, to look for possible security risks and viruses. It is recommended that this review include at least one Supervisor or Project Leader, and one specialized personnel, for proper risk evaluation.

Minimize the exchanging of diskettes. Diskettes is one of the favorite ways of virus spreading. If you need to import one file from another machine, transmit it via electronic mail. This minimizes the probabilities of infection.

Whenever an external diskette is being introduced in your machine, scan it with your anti-virus program to detect any virus and always strictly follow the anti-virus instruction in case of detected infections.

Have the anti-virus programs residing in your memory so it can detect any virus at any time.

When downloading software from the World Wide Web (Internet), you should be aware that any software copied into your machine might contain viruses. **DO NOT DOWNLOAD ANY SOFTWARE FROM ANY WWW SITE THAT YOU DO NOT TRUST COMPLETELY.** Also remember that only legal software can be used by TW employees.

In addition, all PC and Mac systems shall use the TW-approved virus protection software to provide both background (periodic "watchdog" monitoring) and proactive (upon mounting of new media) virus detection and removal. Any user observing or suspecting virus behavior must report this event to the Security Officer. For more details see: APPENDIX A: TW Computer Virus Policy and Procedure.

SECURITY AUDITS

There is a tradeoff between a user's right to absolute privacy and the need of system administrators to gather sufficient information to diagnose problems. There is also a distinction between a system administrator's need to gather information to diagnose problems and investigating security violations.

Security Audits must be conducted frequently in order to keep actualized the policy. This procedure may require that the System Administrator or the Security Officer review systems files and configuration whether they are private or not. This means that users absolute privacy can be affected by this practice; however, the System Administrator and the Security Officer must respect the privacy of information

viewed under these circumstances. TW management reserves the right to inspect and manage any and all information resident on communications and computing equipment at any time.

PHYSICAL AUDIT

The objective of the physical audit is to ensure that the TW computer systems, computer rooms, communication "node rooms", and physical plant are in conformance with the requirements of this Security Policy.

The Security Officer shall oversee a physical audit at least once every six months.

Items to be checked include, but are not restricted to, the following:

- door locks and restriction mechanisms.
- secure tape libraries and tape/optical archives.
- computer equipment location and functionality.
- network equipment and functionality.
- fire detection and extinguishing equipment.

SOFTWARE AUDIT

The objective of the software audit is to ensure that the software environment in the TW network and office conform with the requirements of this Security Policy.

The Security Officer shall conduct a software audit at least once every year.

A list of the software to be inspected must be prepared, and updated as new software is added or removed. Prohibited software specifically includes, but is not limited to the following:

- unlicensed commercial software
- prohibited public domain software
- network packet reading/capture software not used by authorized staff for problem resolution

The audit shall also review all accounts for the following:

- validity of the account (if the account has expired or not)
- account inactivity (all accounts not been used over a period longer than six month shall be removed)
- number of log-in failures (this may indicate breaking attempts)
- adequacy of password protection
- default file protections

Any discrepancies found during the audit shall be reported to the VP or CIO in order to resolve the problems with the offending users and systems. Items that can not be resolved by consensus shall be reviewed with the President and the Project Leader or Supervisor affected. An action plan shall be drawn to resolve the security issues as quickly as feasible, based on the level of security risk and ease of implementation.

OPERATIONS AUDIT

On a routine basis, specialized personnel shall monitor:

- remote log-ins
- break-in attempts
- account file (password) modifications
- network database modifications

On a regular basis, the Security Officer shall review:

- disaster recovery procedures
- media storage and disposal
- examine backup procedures to make sure you can recover data from the tapes.
- account security
- check log files to be sure that information which is supposed to be logged to them is being logged to them
- file system security

All suspicious incidents shall be reported to the Security Officer for review and possible action to resolve or avoid potential security issues.

PROCEDURES TO RECOGNIZE UNAUTHORIZED ACTIVITY

MONITORING SYSTEM USE

System monitoring can be done either by a system administrator, or by software written for the purpose. Monitoring a system involves looking at several parts of the system and searching for anything unusual. Some of the easier ways to do this are described in this section.

Logging

Most operating systems store numerous bits of information in log files. Examination of these log files on a regular basis is often the first line of defense in detecting unauthorized use of the system.

- Compare lists of currently logged in users and past login histories. Most users typically log in and out at roughly the same time each day. An account logged in outside the "normal" time for the account may be in use by an intruder.
- Many systems maintain accounting records for billing purposes. These records can also be used to determine usage patterns for the system; unusual accounting records may indicate unauthorized use of the system.
- System logging facilities, such as the UNIX "syslog" utility, should be checked for unusual error messages from system software. For example, a large number of failed login attempts in a short period of time may indicate someone trying to guess passwords.
- Operating system commands which list currently executing processes can be used to detect users running programs they are not authorized to use, as well as to detect unauthorized programs which have been started by an intruder.

Monitoring Software

Other monitoring tools can easily be constructed using standard operating system software, by using several, often unrelated, programs together. For example, checklists of file ownership and permission settings can be constructed (for example, with "ls" and "find" on UNIX) and stored off-line. These lists can then be reconstructed periodically and compared against the master checklist (on UNIX, by using the "diff" utility). Differences may indicate that unauthorized modifications have been made to the system.

Vary the Monitoring Schedule

The task of system monitoring is not as daunting as it may seem. System administrators can execute many of the commands used for monitoring periodically throughout the day during idle moments (e.g., while talking on the telephone), rather than spending fixed periods of each day

monitoring the system. By executing the commands frequently, you will rapidly become used to seeing "normal" output, and will easily spot things which are out of the ordinary. In addition, by running various monitoring commands at different times throughout the day, you make it hard for an intruder to predict your actions.

INCIDENT REPORTING

Users shall report suspected misuse of their accounts or other misuse they may have noticed. This can be done either calling the Security Officer or a system administrator who manages security of the computer system, or by sending an electronic mail to these persons addressing the problems.

Systems administrators who detect suspected activity their primary goal is the protection and preservation of the site facilities and to provide for normalcy for its users as quickly as possible. Attempts will be made to actively interfere with the intruder's processes, prevent further access and begin immediate damage assessment and recovery. This process may involve shutting down the facilities, closing off access to the network, or other drastic measures. An essential part of containment is decision making (i.e., determining whether to shut a system down, to disconnect from a network, to monitor system or network activity, to set traps, to disable functions such as remote file transfer on a UNIX system, etc.). Sometimes this decision is trivial; shut the system down if the system is classified or sensitive, or if proprietary information is at risk. System Administrators should know in advance what action they must take depending of the attack type and the system being attacked.

Once the incident has been contained, it is now time to eradicate the cause. This process and the recovery of the system, shall be done by the System Administrator with the Security Officer.

System Administrators must keep a detailed logs of all the events that occurred during the attacks. Also they must record all the actions taken during the attack. This will aid in the recovery and follow up procedures that must be realized after a security incident has occurred. The Security Officer shall produce and submit to the Location Supervisor a written, top-level, security audit report based on statistical sampling on a periodic basis with a minimum of once per year and shall include a summary of incidents. The report should include the action, the known or possible causes, the hazard or damage and the corrective action. The report must be evaluated by the Location Supervisor and if necessary it should be distributed to other departments and locations so the case can be know, analyzed and alternative solution be proposed among the TW community.

Information Security Policy

A copy of the current version of the Information Security policy for TW is available through the ICT Web site. It is the responsibility of all employees of this site to read, understand, and follow this policy. After reading the policy, please print out this page and return it to Human Resources. If you have any questions concerning the policy, please contact your Supervisor, or the Site Security Officer.

I have read, understood, and agree to comply with the procedures contained within this policy.

Name (Please print) _____ Date _____

Signature _____

TW Computer Virus Policy and Procedure

TECHNOLOGY AND COMMUNICATIONS UPDATE - NUMBER 1

- Recommended Policy for Desktop Virus Protection
- Corporate Standard Anti-Virus Software Products
- Word Macro-Virus Cleanup Procedures

Pursuant to the TW Information Security Policy recently released, the following information is intended to assist responsible parties in their compliance with the anti-virus measures identified in the General Policy. The relevant sections of the Recommended Policy for Desktop Virus Protection below may be adapted directly into the required Site Security Procedures Document. This update also contains instructions on how to access corporate standard anti-virus software products and includes a special section with information on how to deal with recent Microsoft Word Macro Virus outbreaks.

Please direct any questions to José Vicente Ortega at: jvortega@txwes.edu

RECOMMENDED POLICY FOR DESKTOP VIRUS PROTECTION OVERVIEW

The most important aspect of data security for TW information stored on the desktop is that of ensuring against loss of access by legitimate users. Although the owner of the information will want to prohibit access to the information by external (or unauthorized internal) agents, it is unrealistic, under current TW practices for physical site security, to assume that data moved to a personal desktop computer (PC) is secure. Any file or dataset that resides on a PC can be printed, copied to a removable disk, or even contained within a portable PC and then removed from the premises. Unencrypted information on portable media is vulnerable to loss or theft, especially when carried during travel.

Loss of legitimate access can occur in two ways: through physical equipment failure or user error resulting in deleted or inaccessible data, or through active destruction by intruders (either by obtaining illegitimate log-in access to systems or by the surreptitious introduction of destructive programs typically called "viruses").

The impact of the first type of loss (and ultimately the second) can be minimized by a judicious backup and archive procedure for all crucial desktop data. The costly restoration of one machine should be a rare and isolated event. It is the potential for rapid dissemination of a destructive virus to multiple machines and sites that warrants an even more proactive, preventative approach to address the second type of loss.

As the repository of vital TW knowledge and productivity moves progressively from the data center to the desktop and laptop, a consistent implementation of the recommendations below are essential to limit the University's vulnerability to any widespread loss of crucial data.

OBJECTIVES

Protect valuable data and systems

- Prevent infection
- Recover if infected
- Diagnose and limit outbreak

Maximize likelihood of compliance to recommended procedures

- Make procurement and installation simple for users/site Supervisors
- Expedite distribution of required updates

- Minimize intrusion to users productive activities
- Provide financial incentive to use corporate package

Minimize cost to corporation

- Leverage volume usage
- Centralize administrative/procurement costs

STANDARDS

The virus protection package used should score at least as well as the corporate licensed packages in industry virus coverage tests and should offer comparable or superior capabilities in each of the following areas of vulnerability:

1. Periodic full system scan
2. Auto scan of removable media on insertion
3. Boot sector protection and recovery (DOS/Windows only)
4. Macro Virus strains
5. Network file scan on access/download

The selection of a corporate-licensed package affords operational and procurement convenience to the users and financial savings through combined buying power. Adoption of the licensed package by users will also relieve them of the obligation to verify compliance with the required coverage and features. The licensed package will be made available on the Software Distribution Server for the convenience of the user community.

As interoperability of data from such packages is not as crucial as for productivity tools (word processing, spreadsheets, etc.), there is not as much technical drive to be absolutely uniform in implementation of this type of software. The use of a commercially-supported product is HIGHLY recommended.

Service providers (TW ICT) and local desktop support teams should be encouraged to have access to several different packages to provide maximum capability in the event a new virus is not covered by the licensed product.

RECOMMENDED PROCEDURES

The TW Security Policy requires that each TW site have a Site Security Policy, and that the Site Security Policy contain procedures related to virus prevention, detection, and elimination. This standard recommends that the following procedures be included in each Site Security Policy. Any departure from these procedures should be reviewed with the responsible corporate security body before the Site Security Policy takes effect.

Operational Policy

1. Scan all new systems on delivery.
2. Scan all floppies on insertion (including "shrink-wrapped" software).
3. Install network scanner in Internet browser and check all incoming files.
4. Use boot sector protection and always have a recovery copy (DOS/Windows machines only).
5. Scan entire system at least once per month.
6. Load updated virus signatures at least once per quarter.
7. Designated security officer to be notified of any virus infection immediately when discovered.
8. Follow all above procedures on any home PC used to share data with office PC.
9. Server system Supervisor to be responsible to follow same procedures for all server data.

University Distribution and Monitoring Strategy

1. Users acquiring the package from the University distribution server(s) should get the operational policy automatically implemented in standard configuration.
2. Necessary updates to the licensed package will be posted on the University distribution server(s) as often as available from the vendor.
3. A University database of infection events is to be maintained to permit analysis of outbreaks and their sources and to inform periodic assessment of the validity of and degree of compliance with existing policies.
4. Pursuant to No. 3 above, the responsible body for the University Security Policy should review the infection database annually to update this document as needed.

CORPORATE LICENSING AGREEMENT FOR SYMANTEC

To assist Site Supervisors and field personnel to implement the virus protection policy, TW has selected Symantec Corporate Edition as the corporate standard anti-virus package for PC platforms.

Information ONLY can be obtained from Symantec on these software products at:

<http://www.symantec.com>

This selection of software was based on significant experience and product performance.