Network Protection and Information Security Policy

PURPOSE

The purpose of this policy is to establish administrative direction, procedural requirements, and technical guidance to ensure the appropriate protection of Texas Wesleyan information handled by computer networks.

SCOPE

This policy applies to all who access Texas Wesleyan computer networks. Throughout this policy, the word “user” will be used to collectively refer to all such individuals. The policy also applies to all computer and data communication systems owned by or administered by Texas Wesleyan or its partners.

POLICY

All information traveling over Texas Wesleyan computer networks that has not been specifically identified as the property of other parties will be treated as though it is a Texas Wesleyan asset. It is the policy of Texas Wesleyan to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information. In addition, it is the policy of Texas Wesleyan to protect information belonging to third parties that have been entrusted to Texas Wesleyan in a manner consistent with its sensitivity and in accordance with all applicable agreements.

RESPONSIBILITIES

The Chief Information Officer (CIO) is responsible for establishing, maintaining, implementing, administering, and interpreting organization-wide information systems security policies,

standards, guidelines, and procedures. While responsibility for information systems security on a day-to-day basis is every employee's duty, specific guidance, direction, and authority for information systems security is centralized for all of Texas Wesleyan in the Information Technology department. This department will perform information systems risk assessments, prepare information systems security action plans, evaluate information security products, and perform other activities necessary to assure a secure information systems environment.

The Security Manager (person in charge of physical security and individual safety) is responsible for coordinating investigations into any alleged computer or network security compromises, incidents, or problems with the IT Infrastructure Services director. All compromises or potential compromises must be immediately reported to the Information Technology department. The IT Infrastructure Services director is responsible for contacting the Security Manager. System administrators are responsible for acting as local information systems security coordinators. These individuals are responsible for establishing appropriate user privileges, monitoring access control logs, and performing similar security actions for the systems they administer. They also are responsible for reporting all suspicious computer and network-security-related activities to the Security Manager. System administrators also implement the requirements of this and other information systems security policies, standards, guidelines, and procedures. In the event that a system is managed or owned by an external party, the department manager of the group leasing the services performs the activities of the system administrator.

Directors and Deans are responsible for ensuring that appropriate computer and communication system security measures are observed in their areas. Besides allocating sufficient resources and staff time to meet the requirements of these policies, departmental managers are responsible for ensuring that all employee users are aware of Texas Wesleyan policies related to computer and communication system security.

The Dean of Students is responsible for ensuring that appropriate computer and communication system security measures are observed by students. The Dean is responsible for ensuring that all student users are aware of Texas Wesleyan policies related to computer and communication system security.

Users are responsible for complying with this and all other Texas Wesleyan policies defining computer and network security measures. Users also are responsible for bringing all known information security vulnerabilities and violations that they notice to the attention of the Information Technology department.

System Access Control

End-User Passwords

Texas Wesleyan has an obligation to effectively protect the intellectual property and personal and financial information entrusted to it by students, employees, partners and others. Using passwords that are difficult to guess is key step toward effectively fulfilling that obligation.

Any password used to access information stored and/or maintained by Texas Wesleyan must be at least 8 characters long, contain at least one uppercase letter and one number or special character.

Passwords will expire annually - every 365 days. When a password expires or a change is required, users should create a new password that is not identical to the last three passwords previously employed.

Passwords stored electronically may not be stored in readable form where unauthorized persons might discover them.

Passwords may not be written down and left in a place where unauthorized persons might discover them.

Passwords may never be shared or revealed to anyone other than the authorized user.

If a password is suspected of being disclosed or known to have been disclosed to anyone other than the authorized user, it should be changed immediately.

Password System Set-Up

All computers permanently or intermittently connected to Texas Wesleyan local area networks must have password access controls. If the computers contain confidential or protected information, an extended user authentication system approved by the Information Technology department must be used. Multi-user systems (servers) should employ user IDs and passwords unique to each user, and user privilege restriction mechanisms with privileges based on an individual's need to know. Network-connected, single-user systems must employ hardware or software controls approved by Information Technology that prevent unauthorized access.

All vendor-supplied default fixed passwords must be changed before any computer or communications system is used in production. This policy applies to passwords associated with end-user user IDs and passwords associated with privileged user IDs.

Where systems software permits, the number of consecutive attempts to enter an incorrect password must be strictly limited. After five unsuccessful attempts to enter a password, the involved user ID must be suspended until reset by a system administrator or temporarily disabled for no less than three minutes. The VPN and Outlook Web Mail constant connections must have a time-out period of 30 minutes and should log out upon reaching the threshold.

Whenever system security has been compromised or if there is a reason to believe that it has been compromised, the involved system administrator must immediately take measures to ensure that passwords are properly protected. This may involve resetting all user passwords and requiring users to change them prior to next system log on.

Whenever system security has been compromised or if there is a reason to believe that it has been compromised, the involved system administrator must take measures to restore the system to secure operation. This may involve reloading a trusted version of the operating system and all security-related software from trusted storage media or original source-code disks/sites. The involved system then would be rebooted. All changes to user privileges taking effect since the time of suspected system compromise must be reviewed by the system administrator for unauthorized modifications.

Logon and Logoff Process

All users must be positively identified prior to being able to use any Texas Wesleyan multi-user computer or communications system resources. Positive identification for internal Texas Wesleyan networks involves a user ID and password, both of which are unique to an individual user, or an extended user authentication system.

Positive identification for all Internet and remote lines involves the use of an approved extended user authentication technique. The combination of a user ID and fixed password does not provide sufficient security for Internet or remote connections to Texas Wesleyan systems or networks. Modems, wireless access points, routers, switches or other devices attached to network-connected workstations located in Texas Wesleyan offices are forbidden unless they meet all technical requirements and have a user authentication system approved by the Information Technology department.

The logon process for network-connected Texas Wesleyan computer systems must simply ask the user to log on, providing prompts as needed. Specific information about the organization managing the computer, the computer operating system, the network configuration, or other internal matters may not be provided until a user has successfully provided both a valid user ID and a valid password.

If there has been no activity on a computer terminal, workstation, or personal computer for a certain period of time, the system should automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the user has provided a valid password. The recommended period of time is 30 minutes. An exception to this policy will be made in those cases where the immediate area surrounding a system is physically secured by locked doors, secured-room badge readers, or similar technology or if the suspended session interferes with the ability of an instructor to complete his/her classroom instructional activities.

With the exception of electronic bulletin boards or other systems where all regular users are anonymous, users are prohibited from logging into any Texas Wesleyan system or network anonymously. If users employ systems facilities that permit them to change the active user ID to gain certain privileges, they must have initially logged on employing a user ID that clearly indicates their identity or affiliation.

SYSTEM PRIVILEGES

Limiting System Access

The computer and communications system privileges of all users, systems, and independently-operating programs such as agents, must be restricted based on the need to know. This means that privileges must not be extended unless a legitimate academic/business-oriented need for such privileges exists.

Default user file permissions must not automatically permit anyone on the system to read, write, execute or delete a system file. Although users may reset permissions on a file-by-file basis, such permissive default file permissions are prohibited. Default file permissions granted to limited groups of people who have a genuine need to know are permitted.

Users with personally-owned computers are responsible for administering a screen saver program securing access to their machine’s hard disk drive, and setting passwords for all

applications and systems software that provide the capability of connecting to Texas Wesleyan resources.

Texas Wesleyan computer and communications systems must restrict access to the computers that users can reach over Texas Wesleyan networks. These restrictions can be implemented through routers, gateways, firewalls, wireless access points, and other network components. These restrictions must be used to, for example, control the ability of a user to log on to a certain computer then move from that computer to another.

Process for Granting System Privileges

Requests for new user IDs and changed privileges must be in writing and approved by the user's manager before a system administrator fulfills these requests. Documents reflecting these requests must be retained for a period of at least one year.

Individuals who are not Texas Wesleyan employees, students, or partners may not be granted a user ID or be given privileges to use Texas Wesleyan computers or networks unless the written approval of a current employee has been obtained and the employee agrees to full responsibility for all activities carried out by the individual(s) she or he is sponsoring. This can be accomplished using the Sponsored Account Request form.

Privileges granted to users who are not Texas Wesleyan employees must be granted for periods of 180 days or less. As needed, users who are not Texas Wesleyan employees must have their privileges reauthorized by the sponsoring department head every 180 days.

Special privileges, such as the default ability to write to the files of other users, must be restricted to those responsible for systems administration or systems security. An exception to this policy may be made if there is a justified business/academic need and permission is acquired through the exception process, using the Exception form. Configuration changes, operating system changes, and related activities that require system privileges must be performed by system administrators.

Third-party vendors must not be given Internet or remote privileges to Texas Wesleyan computers or networks unless the system administrator determines that they have a legitimate business/academic need. These privileges must be enabled only for the time period required to accomplish the approved tasks, such as remote maintenance. If a perpetual or long-term connection is required, then the connection must be established by approved extended user authentication methods.

All users wishing to use Texas Wesleyan internal networks or multi-user systems that are connected to Texas Wesleyan internal networks signify their agreement to comply with all applicable policies by their logon to the network.

Process for Revoking System Access

All user IDs should have the associated privileges revoked after a certain period of inactivity not exceeding 180 days.

If a computer or communication system access control subsystem is not functioning properly, it should default to denial of privileges to users. If access control subsystems are malfunctioning, the systems should remain unavailable until such time as the problem has been rectified.

Users must not test or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the IT Infrastructure Services director. Incidents involving unapproved system hacking, password guessing, file decryption, bootleg software copying, or similar unauthorized attempts to compromise security measures may be unlawful, and will be considered serious violations of Texas Wesleyan policy. Customer/student requests that Texas Wesleyan security mechanisms be compromised must not be satisfied unless the IT Infrastructure Services director approves in advance or Texas Wesleyan is compelled to comply by law. Short-cuts bypassing systems security measures, pranks, and practical jokes involving the compromise of systems security measures are absolutely prohibited.

The privileges granted to users, based on their role within the organization, should be reevaluated by administration annually. In response to feedback from executives, department managers, the Human Resources department, or the IT Infrastructure Services director, system administrators must promptly revoke all privileges no longer needed by users.

Department heads/Directors must report all significant changes in employee duties or employment status promptly to the Information Technology department or system administrators (for non-IT managed systems) responsible for user IDs associated with the involved persons. For all terminations, the Human Resources department must issue a notice of status change to the Information Technology department and all system administrators who might be responsible for a system on which the involved employee might have a user ID.

ESTABLISHMENT OF ACCESS PATHS

Changes to Texas Wesleyan internal networks include loading new software, changing network addresses, reconfiguring routers, and adding remote lines. With the exception of emergency situations, all changes to Texas Wesleyan computer networks must use the formal change management process and be documented in a work order request. In addition, the Request for Change (RFC) must be approved in advance by the Information Technology Infrastructure Services Director except as delegated Emergency changes to networks must be made by persons who are authorized by Information Technology. This process prevents unexpected changes from leading to denial of service, unauthorized disclosure of information, and other problems. This process applies not only to employees, but also to vendor personnel.

Employees must not establish electronic bulletin boards, local area networks, FTP servers, web servers, modem connections to existing local area networks, illegal Peer-to-Peer sharing or other multi-user systems for communicating information without the specific approval of the IT Infrastructure Services director. New types of real-time connections between two or more in-house computer systems must not be established unless such approval is obtained.

Participation in external networks as a provider of services that external parties rely on is prohibited unless Texas Wesleyan legal counsel has identified the legal risks involved and the Chief Information Officer has expressly accepted these and other risks associated with the proposal.

Acquisition of technology services or relying on an external party for network or computing services is prohibited unless Texas Wesleyan legal counsel has identified the legal risks

involved, the Chief Information Officer has expressly accepted these and other risks associated with the proposal, and the service provider meets the security and technology requirements identified by the Information Technology department.

All Texas Wesleyan computers that connect to an internal or external network must employ password-based access controls or an extended user authentication system. Multi-user systems should employ software that restricts access to the files of each user, logs the activities of each user, and has special privileges granted to a system administrator. Single-user systems should employ access control software approved by the Information Technology department that includes boot control and an automatic screen blanker that is invoked after a certain period of no input activity. Portable computers and home/personally-owned computers that contain Texas Wesleyan information are also covered by this policy, as are network devices such as firewalls, gateways, routers, and bridges.

Remote maintenance ports for Texas Wesleyan computer and communication systems must be disabled until the time they are needed by the vendor. These ports must be disabled immediately after use.

Portable devices (smartphones, tablet computers, etc.) using WiFi or commercial data networks should not be used for data transmissions containing confidential personal information unless the connection is encrypted. Such links may be used for electronic communications as long as users understand that confidential personal information must not be transmitted using this technology.

COMPUTER VIRUSES, WORMS, AND TROJAN HORSES

Users must keep approved and current virus-screening software enabled on their computers. This software must be used to scan all software coming from third parties or other Texas Wesleyan departments and must take place before the new software is executed. Users must not bypass scanning processes that could stop the transmission of computer viruses.

Users are responsible for damage occurring because of viruses on computer systems under their control. As soon as a virus is detected, the involved user must immediately call the Information Technology department to assure that no further infection takes place and that any experts needed to eradicate the virus are promptly engaged (817.531.4428).

All personal computer software should be copied prior to its initial usage, and such copies must be stored in a safe place. These master copies can be used for recovery from computer virus infections, hard disk crashes, and other computer problems.

Texas Wesleyan computers and networks must not run software that comes from sources other than business/academic partners, knowledgeable and trusted user groups, well-known systems security authorities, computer or network vendors, or commercial software vendors. Software downloaded from electronic bulletin boards, shareware, public domain software, and other software from untrusted sources must not be used unless it has been subjected to a testing regimen approved by the IT Infrastructure Services director.

DATA AND PROGRAM BACKUP

Personal computer users are responsible for backing up the information stored on their local machines. For multi-user computer (servers) and communication systems, a system administrator is responsible for making periodic backups.

To ensure that valuable or critical data is backed up, it must be stored on network servers managed by the Information Technology department or a trusted partner.

Texas Wesleyan requires the use of industry-standard media, techniques, and timelines in executing all backups. For multi-user computer systems, whenever systems software permits, backups must be performed without end-user involvement, over an internal network and during the off hours.

Storage of backup media is the responsibility of the office computer user or multi-user computer system administrator involved in the backup process. Media should be stored in fireproof safes, at a separate location at least several city blocks away from the system being backed up.

Information listed on the Information Retention Schedule maintained by the Business Office, must be retained for the period specified. Other information must be properly disposed of when no longer needed, which is generally within two years.

Department managers/Directors are responsible for preparing, testing and periodically updating department contingency plans to restore service for all non-IT managed production applications and systems. The Information Technology department is responsible for preparing, testing and periodically updating network service contingency plans.

All Confidential information stored on backup media should be encrypted using approved encrypting methods.

Records, documents and data must not be stored, processed, shared, and/or managed offsite without prior written approval from the Records Retention Officer and Chief Information Officer. This policy includes Cloud services which provide ubiquitous, convenient, on-demand network access to shared resources, such as Apple, Google, Microsoft, and Amazon. Only service providers who a) have been evaluated and approved by IT Infrastructure Services and b) meet all requirements identified within this document may be considered for use.

PORTABLE COMPUTERS

Employees in the possession of portable, laptop, notebook, handheld, tablet and other transportable computers containing Confidential information must not leave these computers unattended at any time unless the information is stored in encrypted form.

Whenever Confidential information is written to a disk or other storage media, the storage media should be suitably marked with as such. When not in use, this media should be stored in a locked safe, locked furniture, or a similarly secured location.

REMOTE PRINTING

Printers must not be left unattended if Confidential information is being printed or soon will be printed. The persons attending the printer must be authorized to examine the information being printed.

Unattended printing is permitted if the area surrounding the printer is physically protected such that persons who are not authorized to see the material being printed may not enter.

PRIVACY

Unless contractual agreements dictate otherwise, messages sent over Texas Wesleyan computer and communications systems are the property of Texas Wesleyan. Administration reserves the right to examine all data stored in or transmitted by these systems. Because Texas Wesleyan computer and communication systems are to be used for business/academic purposes, users are to have no expectation of privacy associated with the information they store in or send through these systems.

When providing computer-networking services, Texas Wesleyan does not provide default message protection services such as encryption. No responsibility is assumed for the disclosure of information sent over Texas Wesleyan networks, and no assurances are made about the privacy of information handled by Texas Wesleyan internal networks. In those instances where session encryption or other special controls are required, it is the user's responsibility to ensure that adequate security precautions have been taken. Nothing in this paragraph must be construed to imply that Texas Wesleyan policy does not support the controls dictated by agreements with third parties, such as organizations that have entrusted Texas Wesleyan with confidential information.

LOGS AND OTHER SYSTEMS SECURITY TOOLS

Every multi-user computer or communications system must include sufficient automated tools to assist the system administrator in verifying a system's security status. These tools must include mechanisms for the recording, detection, and correction of commonly-encountered security problems.

Whenever cost justifiable, automated tools for handling common security problems must be used on Texas Wesleyan computers and networks. For example, software that automatically checks personal computer software licenses through a local area network should be used on a regular basis.

To the extent that systems software permits, computer and communications systems handling sensitive, valuable, or critical Texas Wesleyan information must securely log all significant security relevant events. Examples of security relevant events include users switching user IDs during an online session, attempts to guess passwords, attempts to use privileges that have not been authorized, modifications to production application software, modifications to system software, changes to user privileges, and changes to logging system configurations.

Logs containing computer or communications system security relevant events must be retained for at least three months. During this period, logs must be secured such that they cannot be modified, and such that only authorized persons can read them.

Certain information must be captured whenever it is suspected that computer or network related crime or abuse has taken place. The relevant information must be securely stored offline until such time as it is determined that Texas Wesleyan will not pursue legal action or otherwise use the information. The information to be immediately collected includes the system logs, application audit trails, other indications of the current system states, and copies of all potentially involved files.

Although system administrators are not required to promptly load the most recent version of operating systems, they are required to promptly apply all security patches to the operating system that have been released by knowledgeable and trusted user groups, well-known systems security authorities, or the operating system vendor. Only those systems security tools supplied by these sources or by commercial software organizations may be used on Texas Wesleyan computers and networks. Additionally, only vendor-supported versions of operating systems and applications should be used on production systems. This will generally require periodic upgrades to the current release or the most recent prior version (current -1).

HANDLING NETWORK SECURITY INFORMATION

From time to time, the IT Infrastructure Services director will designate individuals to audit compliance with this and other computer and network security policies. At the same time, every user must promptly report any suspected network security problem, including intrusions and out-of-compliance situations, to the IT Infrastructure Services director or his/her designee.

Provided that no intent to damage Texas Wesleyan systems existed, if users report a computer virus infestation immediately after it is noticed, even if their negligence was a contributing factor, no disciplinary action should be taken.

All network or systems software malfunctions must be reported immediately to the Information Technology department or the involved external service provider.

Information about security measures for Texas Wesleyan computer and communication systems is confidential and must not be released to people who are not authorized users of the involved systems unless the permission of the IT Infrastructure Services director has been obtained. For example, publishing system access information in directories is prohibited.

INFORMATION SECURITY

Risk Identification and Assessment

Texas Wesleyan intends to undertake efforts to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. The IT Infrastructure Services Director will establish procedures for identifying and assessing such risks in each relevant area of the Institution's operations, including:

- **Employee training and management.** The IT Infrastructure Services Director will coordinate with representatives in the Institution's Human Resources and Financial Aid offices to evaluate the effectiveness of the Institution's procedures and practices relating

to access to and use of student records, including financial aid information. This evaluation will include assessing the effectiveness of the Institution's current policies and procedures in this area.

- **Information Systems and Information Processing and Disposal.** The IT Infrastructure Services Director will assess the risks to nonpublic financial information associated with the Institution's information systems, including network and software design, information processing, and the storage, transmission and disposal of nonpublic financial information. This evaluation will include assessing the Institution's current policies and procedures relating to Acceptable Use Policy and Records Management Policy. The IT Infrastructure Services Director will also assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.
- **Detecting, Preventing and Responding to Attacks.** The IT Infrastructure Services Director will evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. In this regard, the IT Infrastructure Services Director may elect to delegate to a representative of the Information Technology Department the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the Institution.

Designing and Implementing Safeguards

The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The IT Infrastructure Services Director will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

Overseeing Service Providers

The IT Infrastructure Services Director shall coordinate with those responsible for the third party service procurement activities among the Information Technology Department and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they will have access. These standards shall apply to all existing and future contracts entered into with such third party service providers.

Adjustments to Program

The IT Infrastructure Services Director is responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program,

as well as any material changes to the Institution's operations or other circumstances that may have a material impact on the Program.

Physical Security Of Computer And Communications Gear

All Texas Wesleyan network equipment must be physically secured. Access to data centers, telephone wiring closets, network switching rooms, and other areas containing Confidential information must be physically restricted.

All employees who must keep Confidential Texas Wesleyan information offsite in order to do their work must possess lockable furniture for the proper storage of this information. At the time of separation from Texas Wesleyan, all Confidential information must be returned immediately.

Exceptions

Texas Wesleyan acknowledges that under rare circumstances, certain users may need to employ systems that are not compliant with these policies. All such instances must be approved in writing and in advance using the Exception process and form.

Violations

Texas Wesleyan network users who willingly and deliberately violate this policy will be subject to disciplinary action up to and including termination, expulsion from the university, and/or legal action.

Terms and Definitions

Access control: A system to restrict the activities of users and processes based on the need to know.

Agents: A new type of software that performs special tasks on behalf of a user, such as searching multiple databases for designated information.

Algorithm: A mathematical process for performing a certain calculation. In the information security field, it is generally used to refer to the process for performing encryption.

Badge reader: A device that reads employee identity badges and interconnects with a physical access control system that may control locked doors.

Booting: The process of initializing a computer system from a turned-off or powered-down state.

Bridge: A device that interconnects networks or that otherwise permits networking circuits to be connected.

Compliance statement: A document used to obtain a promise from a computer user that such user will abide by system policies and procedures.

Confidential information: A sensitivity designation for information, the disclosure of which is expected to damage Texas Wesleyan or its partners.

Critical information: Any information essential to Texas Wesleyan business activities, the destruction, modification, or unavailability of which would cause serious disruption to Texas Wesleyan business activities.

Cryptographic challenge and response: A process for identifying computer users involving the issuance of a random challenge to a remote workstation, which is then transformed using an encryption process and a response is returned to the connected computer system.

Default file permission: Access control file privileges, read, write, execute, and delete, granted to computer users without further involvement of either a security administrator or users.

Default password: An initial password issued when a new user ID is created, or an initial password provided by a computer vendor when hardware or software is delivered.

Dynamic password: A password that changes each time a user logs on to a computer system.

Encryption key: A secret password or bit string used to control the algorithm governing an encryption process.

Encryption: A process involving data coding to achieve confidentiality, anonymity, time stamping, and other security objectives.

End User: An individual who employs computers to support Texas Wesleyan business/academic activities, who is acting as the source or destination of information flowing through a computer system.

Extended user authentication technique: Any of various processes used to bolster the user identification process typically achieved by user IDs and fixed passwords, such as hand-held tokens and dynamic passwords.

Firewall: A logical barrier stopping computer users or processes from going beyond a certain point in a network unless these users or processes have passed some security check, such as providing a password.

Front-end processor (FEP): A small computer used to handle communications interfacing for another computer.

Gateway: A computer system used to link networks that can restrict the flow of information and that employ some access control method.

Hand-held token: A commercial dynamic password system that employs a smart card to generate one-time passwords that are different for each session.

Information retention schedule: A formal listing of the types of information that must be retained for archival purposes and the time frames that these types of information must be kept.

Isolated computer: A computer that is not connected to a network or any other computer. For example, a stand-alone personal computer.

Logon banner: The initial message presented to a user when he or she makes connection with a computer.

Logon script: A set of stored commands that can log a user onto a computer automatically.

Master copies of software: Copies of software that are retained in an archive and that are not used for normal business activities.

Multi-user computer system: Any computer that can support more than one user simultaneously.

Password guessing attack: A computerized or manual process whereby various possible passwords are provided to a computer in an effort to gain unauthorized access.

Password reset: The assignment of a temporary password when a user forgets or loses his or her password.

Password-based access control: Software that relies on passwords as the primary mechanism to control system privileges.

Password: Any secret string of characters used to positively identify a computer user or process.

Positive identification: The process of definitively establishing the identity of a computer user.

Privilege: An authorized ability to perform a certain action on a computer, such as read a specific computer file.

Privileged user ID: A user ID that has been granted the ability to perform special activities, such as shut down a multi-user system.

Router: A device that interconnects networks using different layers of the Open Systems Interconnection (OSI) Reference Model.

Screen blanker or screen saver: A computer program that automatically blanks the screen of a computer monitor or screen after a certain period of inactivity.

Security patch: A software program used to remedy a security or other problem, commonly applied to operating systems, database management systems, and other systems software.

Sensitive information: Any information, the disclosure of which could damage Texas Wesleyan or its business associates.

Shared password: A password known by or used by more than one individual.

Software macro: A computer program containing a set of procedural commands to achieve a certain result.

Special system privilege: Access system privileges permitting the involved user or process to perform activities that are not normally granted to other users.

Suspending a user ID: The process of revoking the privileges associated with a user ID.

System administrator: A designated individual who has special privileges on a multi-user computer system, and who looks after security and other administrative matters.

Terminal function keys: Special keys on a keyboard that can be defined to perform certain activities such as save a file.

User IDs: Also known as accounts, these are character strings that uniquely identify computer users or computer processes.

Valuable information: Information of significant financial value to Texas Wesleyan or another party.

Verify security status: The process by which controls are shown to be both properly installed and properly operating.

Virus screening software: Commercially-available software that searches for certain bit patterns or other evidence of computer virus infection.

RELATED DOCUMENTS

Acceptable Use Policy
Records Management Policy