University of Central Oklahoma

Information Security Policy

UNIVERSITY OF CENTRAL OKLAHOMA
Security Policy, Guidelines and Plan

Table of Contents

Information Security Policy

Introduction

Information is a critical asset, comparable to other assets in that there is a cost to obtaining and storing it and there is value in using it. The Office of Information Technology is committed to protecting the University of Central Oklahoma; its students, faculty and staff; and its partners from knowingly or unknowingly using technology illegally or through damaging actions.

Technology-related systems, including but not limited to equipment, hardware, software, operating systems, storage media, network, and accounts providing electronic mail, WWW browsing, and other applications are the property of University of Central Oklahoma. These systems are to be used for university purposes in serving the students and the UCO community in the course of normal operations.

Effective security is a team effort involving the participation and support of every University of Central Oklahoma students, faculty & staff and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The University of Central Oklahoma has the responsibility for securing its computing and networking systems (both academic and administrative) against unauthorized access, while making the systems accessible for legitimate academic and administrative uses. This responsibility includes informing persons who use the UCO computer and network systems of expected standards of conduct and encouraging their application. It is important for the user to practice ethical behavior in computing activities because the user has access to many valuable and sensitive resources; and the user's computing practices can adversely affect the work of other people. Improper use and abuse of the technology, including networks will not be permitted.

Description

The Office of information Technology (OIT) has central responsibility for the University's information and technology security; and is, therefore, the central source for the University audit and control of data and information technology. The Office of Information Technology is cognizant that increased autonomy and flexibility results in decreased security. Essential to protection of the University's hardware, software, network, and information, are clearly defined and communicated standards. The policies, guidelines, procedures and plan herein will serve as the University's standards.

Scope

The policy governs all aspects of hardware, software, communications, data, and information. Security, control, and audits cover all levels of University students, faculty, staff, and contractors or other entities (herein referred to as *entity*) who may be given permission to log in, view, or access the University's information.

The University will not guarantee the privacy or integrity of user's files or data, but will use its best efforts to protect the integrity of individual user accounts, data, and files from access and use by unauthorized persons. The University does not routinely review user data and files, however, in cases of system failure and subsequent repair or where there is reason to believe there has been unauthorized use or misuse of computer resources, authorized technology personnel, UCO Department of Public Safety personnel and administrative personnel of the University shall have the authority and right to review and audit individual user files, including email. Individual user files may also be reviewed, audited or searched when subject to court order, subpoena or other process of law. Periodic audits of access privileges are conducted.

Guidelines

Guidelines are provided to assist each entity in understanding and implementing the security policy at his/her respective level or position.

Plan and Procedures

The plan and procedures are elaborated to describe the University's intention and implementation of the security policy. These outline the methodology by which University officials will ensure, to the best of their ability, that sensitive and private information is protected.

Penalty for Policy Violation s

Disciplinary action for violating the policy shall be governed by, but may not be limited to, the applicable provisions of student handbooks, faculty handbook and employment handbook, policies of the University of Central Oklahoma, Regional University System of Oklahoma, the Oklahoma State Regents for Higher Education, statutes and regulations of the state of Oklahoma and federal law.

Entities who are in violation of the security policy will lose access privileges to the University's data, Internet, intranet, computing services and networking systems until remediation to University security standards have been met and approved. Additionally, any entity in violation may be subject to disciplinary action possibly including suspension, termination, or expulsion and possible civil and/or criminal prosecution to the full extent of the law.

Policy Revisions

The policy may be viewed on the web at http://technology.ucok.edu/oit/policies.htm

Policy revisions will be announced using the then current most acceptable form of mass communication. The revisions schedule may be found on the last page of this document.

The ***State of Oklahoma Information Security, Policy, Procedures and Guidelines*** are incorporated with this policy by reference.

Implementation

All offices campus wide are responsible for access to their systems. It is the responsibility of each campus entity to ensure security policies are properly followed.

Audit

Purpose

To provide the authority for designated members of University of Central Oklahoma Office of Information Technology Security Team to conduct a security audit on any system at University of Central Oklahoma.

Scope

Accountability. Various offices campus wide are both responsible for access to their systems and accountable to the University and the stakeholders. Each of these offices has a designated person/position who is considered the responsible party for that system. Those individuals/positions are defined within this document.

Policy Updates. It is the responsibility of each campus entity to ensure security policies are properly followed. Policies are reviewed annually. The review will be conducted by the Office of Information Technology with cooperation of the campus departments.

The Office of Information Technology coordinates technology audits which are performed internally, and by external entities such as the Regional University System of Oklahoma, and the Oklahoma Office of State Finance.

Policy Elements

Audits may be conducted to:

1. Ensure integrity, confidentiality and availability of information and resources
2. Investigate possible security incidents
3. Ensure conformance to University of Central Oklahoma security policies
4. Monitor user or system activity where appropriate

Guidelines

For the purpose of performing an audit, any access needed will be provided to designated members of University of Central Oklahoma Office of Information Technology Security Team and/or security consultants or auditors. This access may include:

1. User level and/or system level access to any computing or communications device
2. Access to information (electronic, hard copy, etc.) that may be produced, transmitted or stored on University of Central Oklahoma equipment or premises.
3. Access to work areas (labs, offices, cubicles, storage areas, etc.)
4. Access to interactively monitor and log traffic on University of Central Oklahoma networks.

Information Sensitivity Policy

Protecting Information

Protection of information is governed by legislation, regulatory protections, rules, policies, and procedures of the federal government, the state, the RUSO Board of Trustees, the OSRHE, and the University. Release of information is strictly for UCO related purposes. Confidentiality is compromised when knowingly or inadvertently, information crosses the boundaries of job related activities.

The University requires individuals to adopt best practices in protecting data, especially information which should remain confidential. The University Data Classification system may be helpful in determining the level of protection necessary for information under an individual's purview.

Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of The University of Central Oklahoma without proper authorization. Associated with this policy are guidelines for data classification.

As a public agency we consider most, but not all, documents to be public documents. Data speaks to elements within documents, rather than the total document. This policy acknowledges that even when we discuss public records data, we still need to identify some level of control. Even public data needs to have some level of protection.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect The University of Central Oklahoma Confidential information (e.g., The University of Central Oklahoma Confidential information should not be left unattended in conference rooms or on desks). *Please Note: The impact of these guidelines on daily activity should be minimal.*

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to the Office of Information Technology

Scope

All The University of Central Oklahoma information is categorized into four main classifications. The first three constitute *confidential* information. These classifications are entitled

Classified
Private
Official Use Only
Public

Policy

The University of Central Oklahoma Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to the University of Central Oklahoma or its systems.

Confidential and Non-public Information

The University of Central Oklahoma confidential information designated as Classified, Private, and Official Use Only, contains all information that is not otherwise identified as free and open to the public. The data classification system is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner.

Third-Party Confidential Information

A subset of The University of Central Oklahoma Classified information is "The University of Central Oklahoma Third Party Confidential" information. (See Appendix) This is confidential information belonging to or pertaining to another corporation which has been entrusted to the University of Central Oklahoma by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from proprietary research, joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we have connected a supplier / vendor into The University of Central Oklahoma's network to support our operations.

The University of Central Oklahoma personnel are encouraged to use common sense judgment in securing The University of Central Oklahoma Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact his/her manager.

Generally, all non-public University information must at a minimum reside and be

accessed from a system that is able to provide and enforce varying levels of security access (i.e. read only, inquiry only, read/write, create, update, delete, execute, and copy); reside and be accessed from a system that automatically logs and can report successful and unsuccessful access attempts; be protected through best-practice backup and restore procedures and disaster recovery plans. Confidential information shall not be stored on desktop systems, laptops nor removable devices.

Guidelines

Data Classification

The Data Classification Guidelines provide details on how to protect information at varying sensitivity levels. Use these guidelines as a reference as the University of Central Oklahoma Confidential information in each classification category may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the University of Central Oklahoma Confidential information in question.

Marking Guidelines

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "The University of Central Oklahoma Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "The University of Central Oklahoma [classification category]" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, The University of Central Oklahoma information is presumed to be "the University of Central Oklahoma Confidential" unless expressly determined to be the University of Central Oklahoma Public information by a University of Central Oklahoma employee with authority to do so.

University of Central Oklahoma employees, contractors, people with a business need to know may be granted access to UCO information.

Storage Guidelines. UCO follows a Clear Screen/Clear Desk policy. Keep non-public data from view of unauthorized people. For example: erase whiteboards; do not leave in view on desk or tabletop; lock desktop computer screens and workstations with secure passwords.

Machines should be administered with security in mind. Electronic information should have individual access controls where possible and appropriate. Information must reside and be accessed from a system that is able to provide and enforce varying levels of security access (i.e. read only, inquiry only, read/write, create, update, delete, execute, and copy).

Distribution for each sensitivity level is described in the data classification section.

Disposal/Destruction. Disposal and destruction of UCO documents follow state of Oklahoma regulations and guidelines. Deposit outdated paper information in specially marked disposal bins on the University of Central Oklahoma premises. Electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Data Classification

Public information can be freely shared with individuals on or off campus without any further authorization by the appropriate Information Owner/designee. (Low Risk)

Internal information can be shared with designated members of the University community. Sharing such information with individuals outside of the University community requires authorization by the appropriate Information Owner/designee. (Moderate Risk)

Confidential information can only be shared on a "need to know" basis with a limited number of individuals who have been identified by the appropriate Information Owner/designee or by the Information Security Governance Board. Confidential information includes information that is protected under government, Regents, or university regulation. Controlled use. (High Risk)

Software and Data Security Controls

Data controls are required for integrity and provide information for audit trails used for appropriate management of information processing systems. The security of software and data are as equally important as the hardware if not more important. Software and data can be moved to hardware at other locations and the processing can continue. Obviously even the best hardware is useless without software or data. Many of the hardware security and controls also furnish a safety net for the software and data. The nature of data stored on tape, disks, NAS, SAN, and in memory require additional security and control that hardware security and control cannot provide.

Software security and controls are becoming more complex because of necessity. This necessity is driven by the vulnerability for more numerous methods of breaching software and data security. Therefore, software must have controls developed to provide security and be used at all times. Data should be protected and controlled at the user manager level. For example, the Comptroller is responsible for all financial user systems; the Director of Human Resources is responsible for control of human resources systems; the Registrar is responsible for student information system, for the degree audit system, and for the financial aid system. In the library, the Director of Technical Services is responsible for user access and control.

Software and data endangerment comes from more than one source. The sources can be internal or external. The maintenance of software security is an ongoing process. UCO

will not rely on one line of defense for software security. Challenges to software and information protection are as follows:

Human data entry

Human error is by far the most common, and it is internally generated. This cannot be totally eliminated, but can be reduced by the following:

Identification size. The longer the stream of numbers, the greater the chance for error. Less errors are incurred when the numbers are grouped in three or four number sets. The US government issues a social security number comprised of a nine-number code. It is grouped as a three-number set, a two-number set, and a four-number set.

Check digits should be used by computers systems as part of the input edit programming routine.
Alpha characters can also assist miscoding and provide a larger selection than one number with a range of zero to nine

Have the coding identify something as part of the code.

Application Development Standards

Individuals and application developers who create databases, programs, reports, and other electronic documents must ensure their programs contain the following security precautions.

Applications:
- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support encrypted authentication (e.g. LDAP; Active Directory)

Programming errors

Programming errors are the second largest source of software problems. UCO prefers software designed with built-in program protections which includes but is not limited to systems which edit the input. Following are programming rules that can be followed to reduce error rate.

Naming conventions. UCO has an established data dictionary which defines:
- The title of the data element.
- The size of the data element (now four is used for the year).
- Is the data element alpha, numeric, or alpha-numeric?

- The level of security. Note. Number of security levels and security criteria by level are defined by the system users in cooperation with the programming staff as allowed by the system.
- A program used list. These are programs that use the data element. The data elements are defined as input or output data.
- Authority table. This a list of those UCO positions who have authorization to: access the data, change the data value, and remove the data element value.

Program debugging.

The programming staff will set up test data to ensure that the output is correct for the input data into the program. End users are asked to provide test data material. In most cases the software compiler has a tracing utility program that will be utilized.

One person should be responsible for major test data. This should be the person most familiar with the intended operating system. Past data will identify uninspected input data. The expected results should be jointly predetermined by the user and the programming staff.

Software affecting monetary transactions, items of monetary value, and student or personnel records, that is being written, modified, or updated will be subject to reviews for the required controls.

Systems testing.

Error-free operation indicates programming is complete. The testing should start with very simple test data. With precomputed results, monitor or printer formatted results should compare with the actual ones run. As each level of testing is completed, more complex test data is used.

Data Access

User Program and Data Access

Unauthorized software or data access can be avoided or at least minimized by adhering to the following management guidelines. (See also: Password Policy)

- Authorized user access to the system should be controlled and monitored at all times.
- Managers responsible for administrative applications will authorize user access to their respective systems.
- Bypassing security procedures is restricted.
- Once a program has been written, tested, and received by computer operations, it is the sole property of operations, and no unmonitored access to the program code is

available online to the programmers.
- After three failed attempts, user accounts will be locked for a period of four hours. System administrators or user managers with security access may override the lock if authorized by the user system manager.

Programmer Program and Data Access

- Programmers access is monitored through review of automated logs each week.
- Changes to source code reviewed through automated logs each week.
- Programmers are tracked through automated logs which indicate when they log on to users systems such as human resources, finance, financial aid, degree audit.
- Program and data protection from virus and other deliberate programming malfunctions
- All new software, regardless of the source, will be tested for any form of virus before it is loaded onto the system.
- Any downloaded data that is not from a company source will be screened for virus.

Information Transmission

LANs, WANs, direct telephone dial-in, and the Internet have become information highways for data and software transmissions. There are needs for the encryption of transmitted data. Also, viruses have been known to be passed along these highways.

Access to a computer system that is capable of communicating can be a victim of another computer in any part of the world. The more transmitted information becomes a valuable commodity, the more it should be protected. There are computer hackers out there who are looking for challenges and the only reward they hope to obtain is to access a well-defended system. Therefore, it should be a policy for top management to not brag publicly about how impregnable their computer system is. It only offers a challenge for the uncounted number of hackers who would be willing to stay up nights to prove University personnel were wrong.

Cost analysis

The cost must be compared to the benefit of the security system. The costs include the reduction of the system's rate of transmission, the cost of the system, time required for an Office of Information Technology employee to police the system and protect the encryption key, etc.

Installation procedure.

There is a sequence of events for introducing cryptography to information systems. The following procedures were used in determining the method of securing the UCO networks.

- Select what must be protected.
- Define the quantity of the data and software to be protected.
- Determine transmission locations (to and from)
- Determine the communication media
- Research available solutions and associated costs of ownership
- Select a system
- Test and debug the system
- Configure the system.
- Convert to the system; after some testing has been done, move up to higher-level security.
- Monitored the network and retain logs for one year

Security post-installation operations

After the security system has been installed, there are some concerns to maintaining the security system. The following concerns and recommendations should be addressed with the security system:

- Continuously update the list of items approved for protection. Remove any items that are not needed and add new items to the list as necessary.
- Review the physical levels of security defined.
- The system should be monitored during classified information transmission.
- Change the key often and at random intervals.
- Encrypt the data both in transmission and storage.
- Keep the unencrypted backup in a locked, fireproof safe. Every year, have the lock rekeyed or the combination changed.
- Segment messages being sent.
- Have regular security checks run on all employees who have access to any part of the security system. The reports will be sent to the audit and control head. He/she will make a copy of the reports for the information systems head in a double-sealed envelope.
- Keys or passwords are stored in a file safe in an encrypted format.
- Track data transmission to ensure that it is not being taped.
- A separate key will be assigned to each data resource that requires security. Keys should be changed randomly and frequently.
- Records of key users will be maintained.

Password Policy

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of data entities or of the University of Central Oklahoma's entire corporate network. As such, all University of Central Oklahoma employees (including contractors and vendors with access to University of Central Oklahoma systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any University of Central Oklahoma facility, has access to the University of Central Oklahoma network, or stores any non-public University of Central Oklahoma information.

Policy

Passwords should never be shared with another person. Nor should a person use his/her own password to log in to an account for another person’s use.

User identifications / log ons and passwords

Process for assigning user ids and passwords varies from system to system based on the capability of the system in place; however where possible within the system, the user manager who is responsible for the application, will add user and assign appropriate security level. For systems in which a system administrator or programmer must add users, authorization is granted in writing by e-mail or memo by user manager.

User IDs and associated passwords give unique security access to an account entrusted to said user who is responsible for all activity in the corresponding account. Therefore user ids and passwords should not be shared. (See Computer and Network Usage Policy).

Where available, user shall be given the authority to change his/her own passwords.

Where available, users will not be given authority to change a password and immediately change it back to its original character string.

Password Protection Standards

Immediately change default user names, identifications, and passwords that are shipped with manufacturer and vendor products.

Do not use the same password for University of Central Oklahoma accounts as for other non-University of Central Oklahoma access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various University of Central Oklahoma access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for a Windows account and a UNIX account.

Do not share University of Central Oklahoma passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential University of Central Oklahoma information.

If someone demands a password, refer them to this document or have them call someone in the Vice President's office.

Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Do password protect the screen saver on the desktop computer, workstation, and laptop. Password protect mobile devices such as thumb drives, memory sticks, CDs, and DVDs.

Change passwords at least once every 120 days (except system-level passwords which must be changed quarterly). The recommended change interval is every three months.

If an account or password is suspected to have been compromised, report the incident to the Office of Information Technology and change all passwords.

The Office of Information Technology Security Team may perform password cracking or guessing may be performed during an audit or on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Password Usage Standards

- Use a new a different password each time the password must be changed; avoid reusing old passwords
- Use unique passwords for each system and account; avoid using the same password for multiple accounts
- Passwords should be protected. Passwords are confidential and should not be shared with others. Select strong passwords that can be remembered to avoid

storing them on paper or other media

- Change passwords when there is a possibility the passwords or the systems have been compromised
- Temporary passwords should be changed immediately
- All system-level passwords (e.g., root, enable, operating system administrative accounts, application administration accounts, etc.) must be changed on at least a quarterly basis.
- System-level passwords are made available to a select few who need access to perform their jobs. An individual may be granted system-level access to one or to multiple systems, based on job requirements.
- All production system-level passwords must be part of the password management system
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every ninety days. Where available through end-user software policy, password changes are forced.
- User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be stored in clear text and must not be stored on mobile devices without encryption and protection.
- Passwords should not be included in any automated log-on procedures
- Avoid reusing or cycling old passwords for at least twelve months.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.
- Passwords will be disabled on mission critical systems if not used for a period of 30 days and on other systems if not used for a period of 60 days
- In systems that allow forced password changes, passwords will expire every 90 days.

Guidelines

General Password Construction Guidelines

Passwords are used for various purposes at University of Central Oklahoma. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Examples of poor or weak passwords include:

- the password contains less than eight characters
- the password is a word found in a dictionary (English or foreign)
- the password is a common usage or easily identified word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "University of Central Oklahoma", "sanjose", "sanfran" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong Passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. NOTE: Do not use either of these examples as passwords!

Keeping Passwords Safe

- Never reveal a password over the phone or in an e-mail message to ANYONE
- Never reveal a password to the boss
- Refrain from talking about a password in front of others
- Hinting at the format or content of a password (e.g., "my family name") is revealing
- Do not reveal a password on questionnaires or security forms
- Family members do not need your work-related passwords
- Co-workers who need access to your accounts while on vacation may follow appropriate access request procedures to get information to cover for you.
- Do not use the "Remember Password" feature of applications (e.g., Web sites, Windows, OutLook, Netscape Messenger).

Access to the University of Central Oklahoma Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

Use of Passwords and Passphrases for Remote Access Users

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"TrafficOnR00T77Wast^fThisMorning"

All of the rules above that apply to passwords apply to passphrases.

Hardware Security

Protection From Human Disasters

The University does not showcase our computer systems. Security is a major concern of the University. Computer systems are likely to be the target of protestors, disgruntled workers, or even terrorists. The decentralization of computer systems, work group systems, and freestanding systems have increased the difficulty of protecting the computers and its information contents.

Human Intrusion

The first consideration is the basic physical requirements and location for security. The human-factor intrusion considerations have been given to the following items.

Computing Facilities. The computer operations building is located away from the main hub of the University grounds. It is located in an area of a building with a minimum of people traffic. The single floor has only one window. The computer site is not located in a high-crime area or in the path of any radar scanning.

Entryway. A triple set of doors made of strong steel with secure locks is the controlled entryway. The first two doors are opened and visitors can be recognized by the receptionist. Visual recognition with proper ID presented enables visitors through the third door only when essential. Visitors including venders are required to sign in and out, even for meetings in the conference room. Staff are required to sign in and out on the staff board.

Additional Technology Facilities. Buildings, rooms, and other locations in which mission critical hardware, software, and equipment are located are secured as high-security access with key, keypad locks, or other secure locking mechanisms. Passcodes to high security areas are changed quarterly.

Natural and Man-Made Disasters

Natural disasters are often defined as acts of God. These environmental disasters are virtually impossible to predict, let alone avoid. Oklahoma is more prone to high winds, water, and tornados than another type of disaster.

Tornados and High Winds (See also UCO Emergency Procedures, published by Department of Safety and Environment). Tornadoes are prone to occur in our area of the country. The following items were determined to be appropriate preparation:

- One story building to house the computer center.
- Windowless, except for entry area.

- Avoid placing any objects that may cause damage to the computer system if it is too close to it.
- Off-site storage is used for mission critical data.
- Have larger than normal diesel-powered UPS systems to carry all the current needed by the system.
- Procedures to shut down and turn off any hardware that is not essential to the system operation. If backup generators are needed to run the system until local power is available, have enough power to furnish lights and the air conditioner.
- Have a cellular phone charged and ready.
- Have two-way radios ready.
- Have a battery-operated radio for weather advisory information.
- Have a safe place for employees to stay until the severe weather warning is over.
- If time permits, the computer system should be turned off when the warning sounds. Backed-up disks and/or tapes should be locked in the safe.

Water . The computer center is not located on a flood plain. Water damage. There are man-made constructions that can damage computer centers that are difficult to foresee. These can result from plugged storm sewers, broken water mains, or roof leakage. Computer operations has been be provided with a priority list of names and telephone numbers to call to notify someone in case of a problem.

Power Failure . A UPS system is plugged into the essential file servers and main computer systems. The other devices may only need surge protectors. There is an automatic computer backup and shutdown within the UPS system. Operations staff has been provided a priority list of names and telephone numbers to call in case of a power failure.

Secondary Electrical Power Supply . The computer complex has its own secondary electrical power supply for lights, computer hardware, and air conditioning operations. There is enough fuel to run the generator for three days. Other units support work group file servers, online key people, etc.

Fire . An updated clean agent fire protection system was installed in 2007. Automatic fire extinguishers in the computer areas are turned on after a 30-second alarm is sounded. Support and Operations personnel have been trained to respond appropriately. They have been provided a priority list of names and telephone numbers to call to notify someone of the event.

General Considerations

The following are items that are available to support the micro-environmental needs:

- Disaster-recovery procedures.
- Remote network file backup site.

- Commercially available computer backup systems.
- Automatic-dial fire or police telephones.
- Do not allow maintenance and customer service engineers in the area without Office of Information Technology personnel present
- Conduct frequent drills of backup systems.
- Do not post signs to make the site conspicuous.
- Conduct emergency drills more than once a year.
- Have portable fire extinguishers throughout the computer complex.
- Have all fire extinguishers checked once a year.
- No smoking in any UCO buildings
- No computer hardware shall be brought into or taken out of the computer area without the approval of the operations supervisor.

Server Security Policy

Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by University of Central Oklahoma. Effective implementation of this policy will minimize unauthorized access to University of Central Oklahoma proprietary information and technology.

Scope

This policy applies to server equipment owned and/or operated by University of Central Oklahoma, and to servers registered under any University of Central Oklahoma-owned [internal] network domain.

This policy is specifically for equipment on the internal University of Central Oklahoma network.

Policy

Ownership and Responsibilities

All internal servers deployed at University of Central Oklahoma must be managed by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by the Office of Information Technology Security Team. Each operational group must establish a process for changing the configuration guides, which includes review and approval by Office of Information Technology Security Team.

Servers must be registered within the university enterprise management system. At a minimum, the following information is required to positively identify the point of contact:

- Server contact(s) and location, and a backup contact with office hours and after hours contact information
- Hardware and Operating System/Version
- Main functions and applications, if applicable
- Information in the university enterprise management system must be kept up-to-date
- Configuration changes for production servers must follow the University's information technology change management procedures.

General Configuration Guidelines

- Operating System configuration should be in accordance with approved Office of Information Technology Security Team guidelines.

- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods.
- The most recent service packs, security patches, critical updates and virus definition files must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and therefore will not be permitted
- Always use standard security principles of least required access to perform a function.
- Do not use administrator/root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers will be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled open access areas.
- Servers will have TCP/IP configured as the only networking protocol
- Servers must have the "domain admins" and "ISTS" groups configured in the local administrators group
- Servers must be in a physical location that is access controlled
- All mission critical servers must be house by the Office of Information Technology

Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security related logs will be kept online for a minimum of 3 weeks.
    - Daily incremental tape backups will be retained for at least 1 month.
    - Weekly full tape backups of logs will be retained for at least 1 month.
    - Full backups will be retained for a minimum of eight weeks.
- All security related logs will be reviewed on a weekly basis by the server administrator/security manager.
- Security-related events will be reported to Office of Information Technology Security Team, who will review logs and report incidents to OIT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

Compliance

- Audits will be performed on a regular basis by the Office of Information Technology Security team and authorized organizations for the University of Central Oklahoma.
- Audits will be managed by the internal audit group or Office of Information Technology Security Team, in accordance with the *Audit Policy*. Office of Information Technology Security Team will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

Mission Critical Servers

The University will purchase vendor products which are identified as Tier I server systems including hardware and operating systems. Systems considered as unsecurable operating systems will not be allowed; therefore, the University will not support them.

Security protection is demonstrated in terms of six standard levels of security for information technology systems. Items listed are representative of the controls at each perceived security level. These control levels are Prevention, Deterrence, Detection, Containment, Maintenance, and Recovery.

Prevention. Hindering or impeding or creating an obstacle to physical and/or logical access to a system.

Physical
Receptionist screens Computer Center visitors during normal business hours
After hours access to Computer Center limited via DPS security and keying systems
Business critical equipment housed in Computer Room
Computer Room
Environmentally controlled computer room with concrete reinforced walls
Temperature, humidity, and water alarms on environmental control equipment
PDU to isolate computer equipment from power source
Fire alarms/fire suppression system are monitored quarterly
Diesel powered UPS with battery backup system housed in secured out building

Data
Access to root login information is limited only to system administrators by designated system
Root passwords are changed at least every quarter and immediately when personnel who had access change jobs or leave the University's employment.
Remote access to root login information is disabled

OIT personnel have unique login information assigned
Access to system administrator accounts is limited to authorized personnel
Departments responsible for Administrative application security:
Finance System: Controller
HR/PR System: Director of Employment Services
Financial Aid System: Director of Financial Aid
Degree Audit System: Enrollment Management Registrar
Student Information System: Enrollment Management Registrar
Library System: Director of Technical Services, Chambers Library

Deterrence. Providing a negative motivational influence or a disincentive to gain access to a system. Discouraging actions or preventing occurrences by instilling fear, doubt, or anxiety.

Physical
Receptionist screens Computer Center visitors during normal business hours
After hours access to Computer Center limited via DPS security and keying systems
Business critical equipment housed in computer room

Data
Passwords required
Passwords changed quarterly
User education on securing/selecting passwords

Detection. The process of discovery that some action occurred or some state exists outside the norm.

Physical
Receptionist screens Computer Center visitors during normal business hours
After hours access to Computer Center limited via DPS security and keying systems
Computer Room
Temperature, humidity, and water alarms on environmental control equipment
PDU to isolate computer equipment from power source
Fire alarms/Fire suppression system

Data
Activate logging systems (error, login, su,etc)
Monitor system processes
Audit system logs

Containment. A system designed to prevent the accidental or intentional release of a foreign routine in hardware or software; keeping a virus, worm, or other unauthorized condition from spreading.

Physical
Fire suppression system

Data
Compromised userids disabled/passwords changed
Remote access disabled until problem resolved

Maintenance. The work or procedures of keeping a system in proper working condition

Physical
Maintenance contracts in place with vendors that support environmental control, fire control, security, and power backup systems
Maintenance contracts in place with computer hardware vendors
Preventive maintenance preformed on hardware (printers, tape drives, etc)
" \f S

Data
Maintenance and licensing contracts in place for all software vendors
Operating systems and software packages maintained at latest release level
Security fixes applied

Recovery. Restoration or returning a system to a former state or better condition

Physical
Maintenance contracts in place with vendors that support environmental control, fire control, security, and power backup systems
Maintenance contracts in place with computer hardware vendors

Data
Maintenance and licensing contracts in place for all software vendors
Regularly scheduled backups of operating systems and data stored at an environmentally controlled storage facility
Maintain documentation required for recovery
System startup/shutdown procedures are documented
Backup restoration procedures are documented
List of vendor contact information
System configuration documented
Data specifications/definitions/layouts documented

Desktop Computing

The University will purchase vendor products which are identified as Tier I desktop systems and laptops including hardware and operating systems. Systems considered as unsecurable operating systems will not be allowed; therefore, the University will not support them.

Purpose

The purpose of this policy is to establish standards for the base configuration of desktop computers and laptops that are owned and/or operated by University of Central Oklahoma. Effective implementation of this policy will minimize unauthorized access to University of Central Oklahoma proprietary information and technology.

Scope

This policy applies to desktop computers and laptops owned and/or operated by University of Central Oklahoma, and to end-user hardware, including peripherals, registered under any University of Central Oklahoma-owned [internal] network domain.

This policy is primarily for equipment on the internal University of Central Oklahoma network.

Policy

Ownership and Responsibilities

All end-user hardware deployed at University of Central Oklahoma must be managed by an authorized operational group that is responsible for supported end-user computing. Approved hardware configuration guidelines are established and maintained by each the Office of Information Technology in conjunction with the UCO_Techs group based on general University business needs and approved by the Office of Information Technology Security Team. Exception purchases outside which change the configuration guides, requires review and approval by Office of Information Technology, Technology Support unit or the OIT Security Team.

Security protection is demonstrated in terms of six standard levels of security for information technology systems. Items listed are representative of the controls at each perceived security level. These control levels are Prevention, Deterrence, Detection, Containment, Maintenance, and Recovery. See Appendix x: Security Policy Definitions for explanation.

<u>Prevention</u>

Physical

UCO personnel should familiarize themselves with the daily routines in their offices, as well as the routines in offices where they frequently interact.

Technology Support staff should make themselves known to UCO departments on a consistent basis, particularly during new employee orientation.

Technology Support staff will wear identification badges when performing field service.. UCO personnel should only allow properly-identified OIT personnel access to their areas for the purpose of support and service.

Some areas on campus, such as labs, contain a high concentration of computers or other electronic equipment. Other areas do not contain a high concentration of electronic equipment, but the housed equipment is highly valuable. In areas such as these, logged and monitored keypad / keycard access should be implemented.

An office door key should not be able to unlock the offices around it. Keys belonging to personnel at the director level and higher may be exceptions.

All technology will be inventoried, tracked, and subject to unannounced inspections.

Any computer connected to the campus network is required to have adequate surge protection. Information Technology will provide a list of supported and recommended equipment.

Data

Only computers with file-level security will be allowed to participate on the campus network.

All desktops and workstations participating on the network are required to use a screen lock password.

On a typical workstation, common access levels include Guest, User, Power User, and Administrator. All users will function within the User context on their local machines at all times. Contingent on approval from Technology Support, temporary exceptions may be granted.

Users will not attempt to elevate their access level within any system. Situations requiring elevated permissions will be requested through the Secure Access Request Form and procedure.

Local Administrator accounts will have unique passwords.

The Guest account will never be used under any conditions.

Users will not provide file sharing from their local machines. If users need to share information with other users on the campus network, the Office of Information Technology will provide a reasonable amount of file space for this purpose on a server.

Disk partitions should be formatted using a file system that provides robust file-level security.

Centralized system policies will be implemented to ensure data security.

Domain administrators will never log into desktops or workstations (other than their assigned machine and laptop) using the administrator account.

Users are encouraged to use a clear screen / clear desk procedure.

Users are encouraged to lock doors and to secure laptops when leaving the office.

Data

Forced logon passwords changes occurred every 90 days.

Screen Saver passwords are encouraged.

Configuration of local machine accounts is standardized.

Where local administrator accounts are used, limited access to these passwords are provided only to authorized employees.

File share and NTFS permissions are set by share owner.

Deterrence

Physical

Staff are encouraged to watch for unusual behavior, especially when someone unknown is carrying a computer system out of an office.

Cameras may be provided.

Locks may be provided.

If an area is unlocked, a staff member needs to be present in that area. If no staff member is available, the area should be monitored remotely.

Where appropriate, a more advanced entry system should be used.

In high-security areas and labs, signs should be posted stating that activity is being monitored for security purposes.
Personnel

Alarms / sophisticated entry systems

Visual cues / warnings (more fear factor)

Data
Local log ins are not provided as a general rule.

End-user security awareness training is provided in each application training class and during CyberSecurity Awareness Month activities.

Password security is controlled at the server level.

Users will be encouraged to be observant, lock doors, etc. Encouragement will be reinforced during orientation and user training.

Username / password policy

Training

Fear factor

Detection

Physical

Staff are requested to be observant about positions of computers, monitors, and keyboards. In rare cases, cameras are provided.

It is everyone's responsibility to be observant of suspicious activity and to report such activity to the proper authorities.

Where appropriate, an entry system should log all access to a given area. UCO DPS will monitor and log alarm activity. All entry system logs should be available to appropriate personnel.

Appropriate personnel should review these logs on a regular basis.

Staff

Alarms

Entry system

Audit

Data

Auditing and monitoring is used on during investigations or periods of concern.

All data on the UCO network is subject to routine monitoring and spot-checks.

Appropriate personnel, determined by Information Technology, should receive training in intrusion detection and analysis.

Monitoring

Audit

Intrusion Detection and Analysis training for administrators

Containment

Physical

There is a limited use of same local administrative password by authorized employees.

An office door key should not be able to unlock the offices around it. Exceptions to this would include secretaries / administrative assistants / DPS.

Data
Local Administrator accounts will have unique passwords.

Maintenance

Physical
Four-year maintenance agreements are required for all desktop and laptop purchases.
UPS / surge / fire equipment will be tested on a regular basis

Data
Current updates, hot fixes, and service packs are forced by electronic policies.
It is every user's responsibility to use scandisk and defrag on a regular basis. Information

Recovery

Backups are the responsibility of the individual users except in rare, designated cases. Asset tags will be recorded electronically within equipment if the equipment is capable. All desktops and workstations will be purchased with an extended warranty.

Data

It is every user's responsibility to back up their data on a regular basis. Information Technology will be responsible for backing up server-based resources within its realm of control. Information Technology will keep five days worth of data.

A user should use one and only one main folder or directory in which their data is stored. This folder should be designated as 'Data' and stored in the root directory.

Mobile Devices

Mobile devices refer to Personal Digital Assistants (PDAs), mobile/cell/smart phones, two-way radios, other wireless, and laptops. Mobile storage devices such as serial hard drives, thumb drives, flash drives, compact discs, and digital video discs are also included.

Prevention

Data

Permissions setting are required on all mobile devices that area capable of using permissions.

Passwords shall be required on all devices that are capable of using passwords. See Password Policy for more information.

All employees should receive security information or training in data security

Employees understand that the use of UCO hardware, software, and/or networks constitutes agreement with the University's policies, especially the security policy

Employee and student information should not be discussed or transmitted over radio frequency devices (this includes cordless and cell phones, radios, walkie-talkies, text pagers, wireless PDAs)

Confidential data shall not be stored on local machines, in e-Mail, on CDs, DVDs, flash drives and other mobile devices.

Physical

Loss – All mobile technology devices owned by UCO should be logged. The log should show the name of the employee the device has been checked out to and the dates checked out. The log should also show the length of time that the device will be checked out to that employee

Theft – UCO assets should not be left in view in automobiles or left out of the immediate control of the employee responsible for the asset
Breakage – Well padded carrying cases should be used for laptops

Deterrence

Data

Permissions – NTFS permissions should be used and be moderately restrictive

Policies - Strictly enforce all policies

Encryption – All data that will be transmitted from or to an off-campus location should be encrypted

Physical

Asset Tagging – All mobile devices should have a bar-code asset tag

Locked/Controlled Access – All devices should be stored in a locked area when unattended.

All employees that will use mobile devices should attend a training class on security and/or read and sign a statement of security policies

Detection

Data

Auditing – audit logging should be enabled on laptops to aid in detection of security breaches

Password Changes – requiring passwords to be changed will aid in the detection of unauthorized usage.

Physical

Random Checks/Inventory – Random verification should be made of asset location, status and consistency with equipment logs.

Containment

Data

Upon detection by IT of a security breach the responsible department should be notified; upon detection by a department of a security breach IT should be notified.

Upon detection of a security breach the device should be removed from use or disabled and any corresponding accounts closed (i.e. cell phone and pager accounts closed) until the device or account can be secured and a review of policies and procedures conducted

Physical

If a physical area breach is discovered appropriate departments (IT, DPS, FM) should be contacted to investigate and secure the location

Upon detection of a security breach a review should be made of relevant policies, procedures and practices

Information Technology will immediately notify the affected departments upon detection a security breach

Information Technology should be immediately notified upon detection of a security breach by an employee or department

Maintenance

Data

Mission critical data should be backed up frequently.

Efforts should be made to keep security fixes and service packs up-to-date on all devices

Physical

Devices should be stored in locked areas when not in use

Recovery

Data

Loss of critical data should be recoverable from backups

Physical

Every attempt should be made to recovery a lost or stolen device

Damaged devices should be repaired if economically feasible

Replacement of lost or damaged equipment will be at the discretion and expense of the department that suffered the loss

Networking Policy

Purpose

The purpose of this policy is to establish security standards for networking equipment and network usages. This document describes a required minimum security configuration for all routers and switches connecting to a university network or used in a production capacity at or on behalf of University of Central Oklahoma.

Scope

This policy covers remote access to UCO resources and infrastructure including but not limited to, hardware, cabling plant, building wiring, ethernet, etc. All routers and switches connected to University of Central Oklahoma networks are affected.

Policy

Only authorized equipment may be connected to the University of Central Oklahoma network.

Every router must meet the following configuration standards. Most switches now have router capabilities.

Routers are secured in high-security closets.

Routers use secure access.

Local accounts are provided only for the network security personnel.

Remote account access is limited by IP address

Remote sessions are logged and authenticated.

Strings are stored in an encrypted file.

Access levels are controlled by roles.

Passwords are changed every 90 days.

Vendor defaults are disabled and routers are configured as necessary for the University of Central Oklahoma specific business needs.

Web services are not running on the router

Access policies are enabled to limit to IP addresses and services and connection access is controlled for SSH, SNMP, Telnet, tFTP and FTP

The router is included in the university enterprise management system with a designated point of contact.

Secure OS is enabled on all switches to disable unsecured services.

Each router must have the following statement posted in clear view: "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."

Networking equipment will be secured in the following manner:

Prevention

Redundancy

Secure Environment Servers / Communications Closets

Environmental Controls (Alarm, Temperature, Humidity, Drainage, UPS, Fire Prevention)

Policies / Enforcement of Policies

Deterrence

Firewall

Network Address Translation

Virtual Private Networks

Client/Server Encryption

SSL

Security Dynamics (Changing Password Service)

Detection

Simple Network Management Protocol (SNMP) Traps, Alarms

Pager Notification Software
Logs

Management Server

Radius Server

Regular Scheduled Audits

Security Alarms

Containment

Multiple Areas of Control

Anti Virus Software for Applications e-mail, file/print services

Anti-Virus Management Server

Maintenance

Management Servers

Maintenance Contracts

Spares

Crash Kits

Software Updates

Firmware Updates

Hardware Updates

Recovery

Network Documentation

Disaster/Recover Procedures

Backups

Off-Site Storage

Telecommunications

The purpose of this policy is to outline security approaches for the University's primary voice communications devices and services including but not limited to the Definity switch, voice mail, E911, call accounting and mobile telephones, where appropriate.

Prevention

Passwords shall be required on all devices. See Password Policy.

The telephone switch is on a UPS that is connected to a generator.

Deterrence

All telecommunication rooms should be locked at all times. Access doors to telecommunications department require special key for entry. Only authorized personnel have keys to the Telecommunications space.

Silent alarms are on door access. All systems have reporting alarms.

Enforce strict password policies.

Detection

History log shows unauthorized attempts.

Staff performs random checks of alarms and logs.

Containment

When a security breach is discovered the appropriate department (IT, DPS) should be contacted to investigate.

Maintenance

Data is being back up daily.

Alarm reports checked.

Area is kept dust free through climate control.

Recovery

Back up tapes are located off premise.

A crash kit is stored on the premises for emergencies.

Videoconferencing and Distance Learning Technologies

This policy covers all hardware and software that relates to videoconferencing and to interactive distance learning technologies such as Tandberg, Polycom, and Team Stations including networking, applications, user access, microphones, cameras, etc.

Purpose

The purpose of this policy is to ensure security techniques are documented for users and are used by technical staff.

Prevention

Physical

The rooms with videoconferencing equipment and the distance learning classrooms which contain the full-motion video and audio equipment, are always locked unless class is in session or the meeting room is in attended use.

Access to the video conferencing facilities is for authorized users only.

Users will be trained to use the video conferencing equipment prior to class transmittance.

A password is required to obtain access to the video conferencing unit. Video technicians will assist students and others in logging on to the equipment and services.

Users are forbidden to download, install or run software on video conferencing systems without express permission from the Technology Resource Center.

TRC staff are always present when video conferencing equipment is in use.

Video conferencing equipment is turned off when not in use.

Deterrence

No confidential data may be made available/transmitted through video conferencing equipment. Refer to the Information Sensitivity Policy for questions on how to deal with data transmission.

Copyrights must be protected and permission obtained before transmitting copyrighted information through the video conferencing equipment. Contact Academic Affairs or legal authorities for advice and assistance.

Passwords are required for access to video conferencing systems. Passwords are provided to TRC staff.

Administrative user logon and password is needed for authorized downloading, installation and copying of files or software to the Presentation Computer.

Detection

Anyone using this system expressly consents to visual monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to University administrators and law enforcement officials.

Technology Resource Center staff conducts daily review of systems.

All activities in the Video conferencing room will be visually monitored by the Technology Resource Center staff.

All trouble reports received by Technology Resource Center staff will be reviewed for symptoms that might indicate obtrusive activity.

Containment

User education shall be provided in order to train end users on video conferencing systems to report any anomalies in system performance to the Technology Resource Center staff.

Technology Resource Center staff are always on site when equipment is in use.

The purpose of containment is to limit the extent of damage from a problem. An essential part of containment is decision making (e.g., determining whether to disconnect one site, to shut a system down, monitor system or network activity, disable functions, etc.).

In some cases, Technology Resource Center staff may find that it is prudent to remove all access or functionality as soon as possible, then restore normal operation in limited stages.

If there is a technical issue with a receive site - for example excessive feedback during the transmission - that disrupts the instructor and/or the other receiving sites, Technology Resource Center staff will work with the site in any way to solve the issues including scheduling point-to-point test broadcasts, testing with OneNet and any other methods of diagnosis. If after three class transmissions the issue can not be resolved, Technology

Resource Center staff will attempt to find the next closest location for enrolled students and will remove the site from the reservation. The site will not be brought back into the reservation during the duration of the course, but will schedule future course transmissions after the issue has been resolved.

Maintenance

User education shall be provided in order to train end users on the proper shutdown, startup, and system control procedures.

Technology Resource Center staff will work with each site to assure that they are prepared to receive or send class transmissions. This is include scheduling point-to-point test broadcasts, testing with OneNet and various other methods of system diagnosis and preventative maintenance.

Technology Resource Center staff will install software updates/upgrades/patches as they are made available from the vendor.

Virus protection software will be placed on all appropriate machines.

Recovery

User education shall be provided in order to train end users to restore normal operation.

The goal of recovery is to return the system to normal. In general, Technology Resource Center staff believes that bringing up services in the order of demand to allow a minimum of user inconvenience as the best practice.

Technology Resource Center staff will make a master backup VHS tape of any class that is transmitted. This master tape will be used to make duplicates of the transmission for the students to view if there is a technical problem at a receive site, at UCO or with the OneNet system. The tape will be sent to the contact person at each receive site. *These tapes are not a permanent record of class. They are used as a backup procedure in the event of technical problems.*

Documented procedures for system re-installation will be accessible for technicians.

Other

In the follow-up stage, the system will be monitored for items that may have been missed during the recovery and maintenance stages. Continual system monitoring will be conducted to ensure the problem is resolved.

Technology Resource Center staff will perform a postmortem analysis. This analysis will include information related to exactly what happened, and at what times; efficiency and performance of the staff involved with the incident; what kind of information did the staff need quickly; how could they have gotten that information as soon as possible; and what would the staff do differently next time.

A report describing the exact sequence of events: the method of discovery, correction procedure, monitoring procedure, and a summary of *lessons learned* will be written.

Internal Lab Security Policy

Purpose

This policy establishes information security requirements for University of Central Oklahoma labs to ensure that University of Central Oklahoma confidential information and technologies are not compromised, and that production services and other University of Central Oklahoma interests are protected from lab activities.

Scope

This policy applies to all internally connected labs and University of Central Oklahoma students, faculty, staff and third parties who access University of Central Oklahoma's labs. All existing and future equipment, which fall under the scope of this policy, must be configured according to the referenced documents. DMZ Labs and stand-alone, air-gapped labs are exempt from this policy. DMZ labs must comply with the *DMZ Security Policy*.

Policy

Ownership Responsibilities

Lab managing organizations are responsible for assigning lab managers, a point of contact (POC), and a back-up POC for each lab. Lab operators must maintain up-to-date POC information with the Office of Information Technology Security Team. Lab managers or their backup must be available around-the-clock for emergencies; otherwise emergency security actions will be taken without their involvement.

Lab managers are responsible for the security of their labs and the lab's impact on the University network and any other networks. Lab managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined lab managers must do their best to safeguard University of Central Oklahoma from security vulnerabilities.

Lab managers are responsible for the lab's compliance with all University of Central Oklahoma security policies.

The Office of Information Technology Security Team reserve the right to interrupt lab connections that impact the university network negatively or pose a security risk.

All user passwords must comply with University of Central Oklahoma's *Password Policy*. In addition, individual user accounts on any lab device must be deleted within three (3) days when the accounts are no longer authorized . Group account passwords on lab computers (Unix, windows, etc) must be changed quarterly (once every 3 months). For any lab device that contains University of Central Oklahoma proprietary information, group

account passwords must be changed within three (3) days following a change in group membership.

General Configuration Requirements

People using labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the University network and/or non-University of Central Oklahoma networks and computers. These activities must be restricted within the lab.

The Office of Information Technology Security Team reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals, physical and software configuration security.

All labs networks with external connections must be approved by the Office of Information Technology Security Team. These labs must not be connected to University of Central Oklahoma university production network or any other internal network directly, via a wireless connection, or via any other form of computing equipment. A waiver from the Office of Information Technology Security Team is required where air-gapping is not possible (e.g., Partner Connections to third party networks).

Training Policy

Technology Resource Center (TRC) staff, while providing deskside and other assistance to clients throughout the UCO community, may have access to confidential and/or secure information. All restrictions placed upon those normally having access to this information will also apply to TRC staff, and the information will not be divulged or recreated in any format.

This policy applies to personnel and the use of training software, assessment, professional development databases, and assistance to client users and departments .

Prevention
Manage passwords appropriately
Physically secure CD-ROMs
Training on password management
Log CD-ROM usage

Deterrence
Audit courses taken through Administrator report menu
Physically secure CD-ROMs
Manage passwords appropriately
Log CD-ROM usage

Detection
Use Administrative Reports to check usage
Periodically check with students to match progress
Monitor usage of courseware/assessment

Containment
Delete unauthorized users
Communicate with vendor to prevent future unauthorized access
Review storage methods
Review local PC security

Maintenance
Ensure all CD-ROMs are up-to-date
Keep subscriptions current
Keep usage log current

Recovery
Contact vendors for replacement CD-ROMs/access codes
Periodically print course progress reports

Information Security Plan

This Information Security Plan ("Plan") describes University of Central Oklahoma's safeguards, to the best of our ability, to protect *covered data and information*.[1] These safeguards are provided to:

- Ensure the security and confidentiality of covered data and information;
- Protect against anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any customer.

This Information Security Plan also provides for mechanisms to:

- Identify and assess the risks that may threaten covered data and information maintained by UCO;
- Develop written policies and procedures to manage and control these risks;
- Implement and review the plan; and
- Adjust the plan to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

Scope of Program

The Program applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the University of Central Oklahoma, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the University of Central Oklahoma or its affiliates. For these purposes, the term nonpublic financial information shall mean any information (I) a student or other third party provides in order to obtain a financial service from the University of Central Oklahoma, (ii) about a student or other third party resulting from any transaction with the University of Central Oklahoma involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person.

Elements of the Program :

Identification and Assessment of Risks to Customer Information

The University of Central Oklahoma intends, as part of the Program, to undertake 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. In implementing the Program, the Program Officer will establish procedures for identifying and assessing such risks in each relevant area of the University of Central Oklahoma's operations, including: UCO recognizes that it has both internal and external risks. These risks include, but are not

limited to:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information
- Compromised system security as a result of system access by an unauthorized person [1]
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties

University of Central Oklahoma recognizes that this may not be a complete list of the risks associated with the protection of covered data and information. Since technology growth is not static, new risks are created regularly. Accordingly, the Office of Information Technology will actively participate and monitor advisory groups such as the Educause Security Institute, the Internet2 Security Working Group and SANS for identification of new risks.

University of Central Oklahoma believes current safeguards are reasonable and sufficient to provide security and confidentiality to data and information maintained by the University. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information. The University community is encouraged to review security "best practices" annually and to follow these guidelines as applicable.

Information Security Plan Coordinators

Director of Risk Management, and the Vice President for Information Technology, have been appointed as the coordinators of this Plan. They are responsible for assessing the risks associated with unauthorized transfers of covered data and information and implementing

[1] *Covered data and information* for the purpose of this policy includes *student financial information* (defined below) required to be protected under the Gramm Leach Bliley Act (GLB). In addition to this coverage which is required under federal law, University of Central Oklahoma chooses as a matter of policy also to include in this definition any credit card information received in the course of business by the University, whether or not such credit card information is covered by GLB. Covered data and information includes both paper and electronic records. *Student financial information* is that information that University of Central Oklahoma has obtained from a customer in the process of offering a financial product or service, or such information provided to the University by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

procedures to minimize those risks to UCO. Internal Audit personnel will also conduct reviews of areas that have access to covered data and information to assess the internal control structure put in place by the administration and to verify that UCO departments comply with the requirements of this policy.

Employee Management and Training

References of new employees working in areas that regularly work with covered data and information (Cashier's Office, Registrar, Development and Financial Aid) are checked. During employee orientation, each new employee in these departments will receive proper training on the importance of confidentiality of student records, student financial information, and other types of covered data and information. Each new employee is also trained in the proper use of computer information and passwords. Training also includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, including "social engineering"[2] and how to properly dispose of documents that contain covered data and information

Each department responsible for maintaining covered data and information is instructed to take steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures. Further, each department responsible for maintaining covered data and information should coordinate with the Legal Services department on an annual basis for the coordination and review of additional privacy training appropriate to the department. These training efforts should help minimize risk and safeguard covered data and information security.

Physical Security

UCO has addressed the physical security of the University's covered data and information by limiting access to only those employees who have a business reason to know such information. For example, personal customer information, accounts, balances and transactional information are available only to UCO employees with an appropriate business need for such information.

Loan files, account information and other paper documents are kept in file cabinets, rooms or vaults that are locked each night. Only authorized employees know combinations and the location of keys. Paper documents that contain covered data and information are shredded at time of disposal.

Information Systems

[2] "Social Engineering" occurs when an individual improperly obtains personal information of university customers so as to be able to commit identity theft. It is accomplished by contacting the University, posing as a customer or someone authorized to have the customer's information, and through the use of trickery and deceit, convincing an employee of the University to release customer identifying information.

Access to covered data and information via UCO's computer information system is limited to those employees who have a business reason to know such information. Each employee is assigned a user name and password. Databases containing personal covered data and information, including, but not limited to, accounts, balances, and transactional information, are available only to UCO employees in appropriate departments and positions.

Access is provided to appropriate personnel through a request on a Security Access Request form. Supervisors must approve access for the employee to data access that is being requested. The Office of Information Technology provides access to the data base and forwards the request to system security agents (functional managers who "*own*" the data). System Security Agents grant access at the appropriate level based on the employee's and his/her supervisor's approved request.

UCO will take reasonable and appropriate steps consistent with current technological developments to make sure that all covered data and information is secure and to safeguard the integrity of records in storage and transmission. Office of Information Technology requires that all servers must be registered before being allowed through UCO's firewall, thereby allowing Office of Information Technology to verify that the system meets necessary security requirements as defined by Office of Information Technology policies. These requirements include maintaining the operating system and applications, including application of appropriate patches and updates in a timely fashion. User and system passwords are also required to comply with the University of Central Oklahoma Password Policy. In addition, an intrusion detection system has been implemented to detect and stop certain external threats, along with an [Incident Response Policy] for occasions where intrusions do occur.

When commercially reasonable, encryption technology will be utilized for both storage and transmission. All covered data and information will be maintained on servers that are behind UCO's firewall. All firewall software and hardware maintained by the Office of Information Technology will be kept current. Office of Information Technology has a number of policies and procedures in place to provide security to UCO's information systems. These policies are available upon request from the Office of Information Technology.

The University of Central Oklahoma uses a unique identifier, known as the UCO ID. The identifier is a ten-character number which begins with an asterisk (*) and is automatically generated at the time a "person record" is created.

Management of System Failures

Office of Information Technology has developed written plans and procedures to detect any actual or attempted attacks on UCO systems and has an incident response policy which outlines procedures for responding to an actual or attempted unauthorized access to

covered data and information. This policy is available upon request from the Office of Information Technology.

Selection of Appropriate Service Providers

Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that UCO determines not to provide on its own. In the process of choosing a service provider that will maintain or regularly access covered data and information, the evaluation process shall include the ability of the service provider to safeguard confidential financial information. Contracts with service providers may include the following provisions: An explicit acknowledgment that the contract allows the contract partner access to confidential information;

- A specific definition or description of the confidential information being provided;
- A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- An assurance from the contract partner that the partner will protect the confidential information it receives according to commercially acceptable standards and no less rigorously than it protects the University's own confidential information;
- A provision providing for the return or destruction of all confidential information received by the contract provider upon completion or termination of the contract;
- An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles UCO to terminate the contract without penalty; and
- A provision ensuring that the contract's confidentiality requirements shall survive any termination agreement.

Continuing Evaluation and Adjustment

This Information Security Plan will be subject to periodic review and adjustment. The most frequent of these reviews will occur within Office of Information Technology, where constantly changing technology and evolving risks mandate increased vigilance. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the designated Information Security Plan Coordinators who will assign specific responsibility for Office of Information Technology implementation and administration as appropriate. The Coordinators, in consultation with the Legal Services Department, will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, the sensitivity of student/customer data and internal or external threats to information security.

Revision History

Policy Created:	August, 2003
Revision 1	February, 2006
Revision 2	April, 2007 (*final approval pending*)
Revision 3	July 16, 2015 (Updated with new proposed Data Classification)