UNT Information Security Handbook

The Information Security handbook contains UNT computing guidelines and policy for UNT faculty, staff and students. This document is available for review and print and is required reading for anyone using UNT computing resources. Departments that work with financial, medical, academic, or any other sensitive information are required to read the security handbook and become familiar with the policies and guidelines listed within. This is a continued effort by The University of North Texas to prevent FERPA, HIPAA, GLBA, DMCA, and Copyright Law infringement.

PDF version of this handbook.

1 Overview

1 Overview

The purpose of this handbook is to help managers and users of information resources gain an understanding of the basic knowledge necessary to protect these resources. Information resources include the procedures, equipment, facilities, software and data which are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information. Gaining knowledge about how to protect these resources can ensure that potential for intrusion, alternation, or loss will be less damaging. This handbook should also be considered a guide for learning best practices for securing information resources - it is a guide to help protect against security breaches, unauthorized or improper access to computing resources, unauthorized disclosure of information, and internal and external threats. The responsibilities of University faculty, staff, and students are presented, and, links to UNT Computing Policies, Guidelines, and Handbooks, as well as links to State and Federal laws have been included to provide a basis for the standards that governed the development of the handbook.

2 Introduction

The University of North Texas depends upon its computer systems and networks in all aspects of its mission, from scheduling classes and registering students to generating employee paychecks. The continued operation of UNT information systems depends upon appropriate levels of information security. Maintaining this security depends on all employees doing their part.

The security of our information cannot be maintained only through hardware and software controls. Our behavior as users of the computer hardware, software, and information also affects the confidentiality, the integrity, and availability of that information. This document gives the university computer user the basic knowledge needed to protect university information and assets from misuse, abuse, unauthorized access or unauthorized disclosure. University assets include the hardware that you use (your office computer, workstations, servers, etc.,) software (operating systems, desktop software, etc.,) and information that the hardware and software allow you to access. Such information may be sensitive or confidential and may have policies or laws that protect its availability, integrity, and confidentiality.

Federal and state laws, network by-laws, and organizational policies tell us how to behave in accordance with security measures. Several tell us, more specifically, what is appropriate and expected. Relevant UNT polices include:

- Computer Use Policy (http://www.unt.edu/policy/UNT_Policy/volume2/3_10.html)
- Information Resources Security Policy (http://www.unt.edu/policy/UNT_Policy/volume2/3_6.html)

3 Security Problems

Section 3 - Security Problems

3.1 Sharing Computer Accounts and Passwords

One of the most common security problems that users encounter at UNT is unauthorized use of their computer accounts, generally caused by their sharing their account with a friend or relative. We've had incidents in which an acquaintance used someone's UNT account to charge for purchases using a stolen credit card, or sent a harassing message to someone. Account and password sharing is prohibited in almost any circumstance. You should not log in as anyone other than yourself, and you should not allow anyone to log in as you. Passwords should never be shared, written down, or disclosed to anyone- not even to your supervisor nor should they ever be sent through e-mail. Perhaps you need access another person's electronic files, calendar, etc -- ask your network manager or computer support provider for alternatives. Or perhaps you may need assistance logging in with your university user-id (your EUID)-- contact the Computing and Information Technology Center by calling 565-2324.

Remember, you are responsible for all actions within your account. Your account is like your fingerprint.

3.2 Failure to Protect Confidential or Sensitive Information

Most of us deal with confidential and/or sensitive information on a daily basis. This information might include passwords, social security numbers, performance reviews, student schedules, grades, student payroll information, confidential memos, medical information, credit card numbers, employee payroll information, social security numbers, budgetary/financial information, etc. Do you protect this information? How well do you protect this information? Do you walk away from your computer and leave this type of information displayed on your monitor? Do you leave confidential or sensitive documents on your desk in plain view? Do you leave file cabinets containing this kind of information unlocked? Are sensitive documents locked away after business hours? Do you make comments about confidential information to other employees?

Disclosing information to unauthorized employees, contractors, vendors, parents, etc. prevents the information from being used for its intended purpose and circumvents the controls that have been put in place in order to protect the information. Employees must go through the appropriate training in order to

gain access to some types of information. (For example, the federal law requires that you learn about the kind of student information that can be made accessible. In order to comply with the law, the Registrar's Office offers FERPA training- Federal Educational Rights and Privacy Act- see http://essc.unt.edu/registrar/general/studentferpa.htm for more information about FERPA.) Or, departments require that those who wish to gain access to information or privileges sign statements that the information will be used appropriately. At UNT, University policies require that faculty, staff, and students protect the information that they come in contact with.

3.3 Viruses and Worms

Viruses and worms are malicious programs that generally cause damage to the information stored on your computer and attempt to replicate themselves. A virus attempts to replicate itself to documents and executables on your local computer and resources such as network drives that are connected to your computer. The most common viruses seen in the wild today are Microsoft Office macro viruses. Macro viruses usually arrive attached to a legitimate document and execute as soon as you open the document. Once activated, the virus will replicate itself to all the documents it can find and execute its malicious code such as deleting files or modifying the content of your files. Worms are similar to viruses except that they will attempt to replicate themselves over the network. The most common examples of worms are "email viruses" that arrive as email messages, execute and replicate themselves on the local computer and send copies of the message to people in your address book. Frequently, the viruses and worms don't do their damage right away -- they wait until they have the chance to make copies in other locations before they begin to delete files, etc. Because of this, users may use an infected computer for some time before realizing that a virus is present.

All UNT microcomputers should employ virus protection software to protect against damage from viruses. UNT has a site license for McAfee Virus Protection software. This software package must be updated regularly to be effective. Your departmental network manager should notify you when updates are available -- do not hesitate to install these. In addition, you can reduce your risk of virus infection by following these practices:

- Never open or view email attachments or Instant Messenger (IM) links you are not expecting without verifying the contents from the sender.
- Configure applications such as Microsoft Office to prompt you before executing macros.
- Disable JavaScript and VBScript in email clients and web browsers.

To learn about viruses or for additional information, please refer to UNT's Virus Information Page (http://www.unt.edu/security/antivirus/index.html).

3.4 Hackers

Computer hackers are people who attack or try to gain control over computer systems. For example, a hacker may steal passwords and other secret information, disrupt systems and networks, threaten or vilify others, invade privacy, break into other systems, vandalize, make political statements, or use your computer to set up servers to distribute copyrighted or illegal information. Frequently, experienced hackers will attempt to gain access to a number of systems at once so that their activities are harder to

trace. They may not be stealing your password to access your research data; instead, they merely want to use your computer as a launching point for attacking another computer.

Especially challenging is the fact that hackers invent programs that do their dirty work automatically, and they share these programs with other hackers. A hacker might start a program that searches every system on the Internet for a particular security hole. When the program discovers a machine with that hole, it compromises the machine, installs "backdoors" for future access, and then it proceeds to check other machines. Fortunately, there are several groups of "good guys" who publish information about these activities and how to "patch" the holes. The Computer Emergency Response Team (CERT) at Carnegie-Mellon is likely the most famous.

3.5 People

More common than not, people are more of a threat to security than any other source. People can make mistakes which cause the integrity of data to be questioned, weaken the physical security of computer systems, or even cause systems to crash. Some people intentionally cause security problems. These kinds of people are called hackers but they could also be disgruntled employees.

Other kinds of people weaken security through negligence. These kinds of people share their computer accounts, share their computer passwords, choose bad passwords, don't back-up their files, don't lock their office doors, don't log out when away from their computers, etc.

Then there's the "missing person". This person is unavailable for extended periods due to illness, termination or even death. Can you find important files if your assistant is unavailable? Contingency plans should be made available and kept up-to-date for these kinds of events.

3.6 Lack of Contingency Plans

Disasters can strike at any given moment. Can you confirm that you have adequate plans in place to address how your department (or the areas which you are responsible for) would operate in the event of a fire, flood, tornado, earthquake, loss or unavailability of computer resources, missing personnel, telecommunications outage, etc.? It's important to have contingency plans in place that address how critical operations would continue in the event that one or more important services become unavailable. The plan should provide for short and extended periods when these services are not available. See "Basics of Information Security: Maintaining the Confidentiality, Integrity, and Availability of Information" for more details about contingency plans.

4 The Basics of Information Security

Maintaining Confidentiality, Integrity, and Availability

4.1 Maintaining Confidentiality of Information

4.1 Maintaining Confidentiality of Information

4.1.1 Confidentiality and Open (Public Records)

Most types of university information (records) are defined as either "Confidential" or "Open" (public) within UNT Policy 10.10, the University Records Retention Schedule. Information that is classified as confidential cannot be disclosed or disseminated to the public (people who aren't employees of the university with a need to know this information). Much of the information about our students (grades, financial aid status, Social Security numbers, etc.) is confidential.

4.1.2 Protecting Confidential Information about Students

All of us--faculty members, custodians, administrative assistants, secretaries, computer support staff, vice presidents--have a responsibility to protect information about our students from public disclosure. It doesn't matter whether this information is on the central computer, on a printout, a computer screen, a diskette, a CD-ROM, etc. The Family Education Rights and Privacy Act (FERPA) of 1974, guarantees students the right to protect all information that is not classified as "open directory" information.

Some of the records, other than student records, which are designated as confidential include:

- Apprenticeship Records (Internships)
- Client Records (From Institutes)
- Counseling Notes
- Employee Insurance Files
- Employee Security Records
- Federal Tax Records
- Fines Records, Paid and Unpaid
- Fingerprint Cards
- First Report of Alleged or Occupational Disease
- Investigation Records
- Legal Case Records
- Library Circulation Records
- Medical Records
- Reports- Laboratory
- Request for Name Change- Employee
- Request for Student Transcripts
- Request for Tuition Assistance
- Research Data
- Statement of Truth-in-Lending
- Veterans Administration Records

4.1.3 Protecting Open Directory Information

Open Directory Information about students may or may not be flagged to be "withheld from the public", which means that this information can not be posted on bulletin boards or on websites inappropriately. To be certain that a student's record is not protected check with the Registrar's Office.

The following items are considered open director information for students:

- student's full name
- address (local, permanent, and e-mail)
- University assigned e-mail address
- telephone listing (local, permanent)
- birth date, birth place
- major field of study
- dates of attendance
- degrees and awards received
- most recent previous school attended
- classification
- participation in officially recognized activities and sports
- weight and height of athletic team members
- photograph
- enrollment status (undergraduate, graduate, full-time or part-time)

Some students request that open directory information also be withheld from the public. These students are identified within Enterprise Information System (EIS). Please see FERPA Compliance at UNT or contact the Registrar's Office for additional information (http://www.unt.edu/ferpa/index.html). All UNT employees who regularly deal with student information should attend FERPA training, available through the Registrar's Office. Open directory information includes general information (as listed) but ALL OTHER STUDENT INFORMATION IS CONFIDENTIAL!

4.1.4 Public Information about State of Texas Employees

Unless otherwise restricted, the Texas Public Information Act (also known as the Texas Open Records Act) does not prohibit the disclosure of the records of Texas state agencies- this includes universities. Some information about employees who work for Texas state agencies (including UNT) can be disseminated to the public. This information includes (but is not limited to):

- employee name
- sex
- ethnicity
- salary
- dates of employment
- title

- home and mailing addresses, home phone numbers, social security numbers, or information that reveals whether the employee has family members, except when an employee has indicated in writing that he does not wish this information to be disclosed.

Employees may restrict disclosure of their social security number, home address, and home telephone number, by contacting Human Resources. Requests for information from the public should be referred to the university attorney. See http://www.oag.state.tx.us/AG_Publications/txts/2004publicinfohb_3_01.shtml for more information about the act.

4.1.5 How can you help to ensure confidentiality of information?

- When in doubt don't give it out!
- Identify confidential information as "CONFIDENTIAL" on the print-out pages, diskette, screen, etc.
- Choose good passwords, and keep them secret. Passwords are confidential too!
- Log out and/or lock the office when you're away from your desk.
- Don't permit another person to use your computer account.
- Use special care when posting grades (assign random numbers, don't use part of Social Security numbers).
- Secure print-outs and other documents. Retrieve your print-outs as soon as possible. Don't leave confidential or sensitive documents laying out in plain view.
- Use CONFIDENTIAL paper recycling bins. Make sure discarded diskettes and tapes are unreadable.
- Attend FERPA training- send your student workers too!

4.2 Maintaining the Integrity of Information

Is the information accurate? Is it complete? How do we know?

Unless our information is accurate and complete, it's pretty much useless and it may even be dangerous. Almost all of our data is sensitive in this respect. Grades, salaries, research data, and most other records and documents must be protected from unauthorized modification or destruction. How?

- Check your work for accuracy and completeness.

- Choose good passwords, and keep them secret.
- Log out and/or lock the office when you're away from your desk.
- Don't permit another person to use your computer account.
- Use virus detection/protection software.
- Make sure you have backups (on paper, diskettes, tape, or file server).
- Control (specify, understand, document) who has access to the data that you manage. Control what kind of access they have. Can they update some or all records? Can they update only some parts of a record or all parts of a record?
- Check references when hiring.

4.3 Ensuring the Availability of Information

4.3 Ensuring the Availability of Information

4.3.1 Reacting to a Disaster

Every office should have a contingency plan to address disasters or problems such as fire, theft, water damage, vandalism (including data loss from virus or hackers), loss of key employee, hardware failure, network unavailability, etc. The Computing and Information Technology Center (CITC) must plan for the loss of the enterprise information system and other critical systems needed for the business operations of the University. Other departments must plan how they will cope if their own systems are damaged, or if CITC administered systems are unavailable for an extended period (possibly up to three weeks). Contingency plans should address the most critical functions, such as registering students, paying employees and vendors, disbursing financial aid, etc.

Contingency Plans are basically made up of procedures and lists. Sometimes simple plans are the best and they're certainly better than no plan at all. Procedures should address how to accomplish basic tasks without computers/networks: who does what, what should be done first/second/..., how do you restore files from backup, etc.

Lists should include:

- Names of key personnel (faculty, staff, computer support staff, back-up support, building representatives, safety emergency coordinators, emergency services personnel, etc.)
- key personnel contact information (telephone/cell number, pager numbers, etc.)
- critical data, hardware, and software
- critical documentation

- critical supplies and equipment
- vendor contact information (business name, telephone number, address, contact name, etc.)
- emergency procedures (building coordinator plans, evacuation plans based on type of disaster, test dates, etc.; contact Risk Management for more information)
- storage location of critical back-up data
- date of the last review of all elements of the contingency plan

A contingency plan is never really "finalized." Some of the information in the lists change frequently and should be updated and disseminated. Departments should test their plans periodically to ensure that contingency procedures are still practical, files can be restored, etc. Plans should provide short as well as extended periods when critical resources may be unavailable. See the “Checklist Criteria For Business Recovery” (sponsored by FEMA) guide for more information on developing a contingency plan, http://www.fema.gov/ofm/bc.shtm.

4.3.2 BackUp (Make an Extra Copy Of) Your Files

In the event of a disaster, will you be able to recover the files that have been lost? Your files (electronic data, e-mail correspondence, etc.) should always be backed up (copied) and placed in a secure location- especially those files that you do not use on a daily basis, yet may be critical to your office operations.

Here are a few ideas to help you with the Backup process:

- Add "Backup Files" to your weekly or monthly "to-do" list.
- Know how often the files on your department's file server are backed-up.
- Backup what you can't replace on your hard drive.
- Backup, or "archive" your important e-mail messages (see your computer support person if you need assistance).
- Keep a Backup in a secure location- somewhere other than your office.
- Make use of folders or directories to simplify the Backup chore.
- Use version numbers in filenames, keep several recent versions.
- If you need assistance, contact the computer support person in your department.

4.3.3 Preventing a Disaster

Several measures may actually help to prevent a disaster. These could include:

- Perform regular updates to the contingency plan.
- Perform periodic risk assessments to determine what is vulnerable.
- Have an up-to-date contingency plan in place and distributed to key personnel.
- Make sure your critical files are backed-up up at least once a week.
- Ensure the physical security of your office/computer areas.
- Choose good passwords and keep them secret.
- Log out and/or lock the office when you're away from your desk.
- Do not allow any other person to use your computer account.
- Use virus detection/protection software.

5 Information Safeguards

5 Information Safeguards

5.1 Special Procedures for Securing Sensitive Documents

Many records fall under the provisions of laws and regulations that impose additional security and retention requirements designed to prevent unauthorized access to those records. Examples of such laws are the Health Information Portability and Accountability Act, which regulates access to Protected Health Information, and the Gramm-Leach-Bliley Act, which regulates access to non-public financial information about a University customer (student or other parties purchasing services from the University). The UNT Record Retention Schedule indicates the retention period of these records, but in addition to the retention procedures, users of documents falling under the provisions of those laws and regulations should be aware of the following security guidelines:

- Workstation screens should not be visible to anyone but the authorized user of secure documents
- Workstations used to view or edit secure documents should be protected with a screen saver that requires a password to re-activate the screen after it goes into sleep mode

- Only authorized persons may use a machine on which secure documents are viewed or edited (no sharing of a workstation, in other words.)
- A person with password access to secure data is prohibited from sharing his or her password with others.
- Passwords must be changed periodically in compliance with UNT standards.

State and federal regulations may also require that some or all of the following access monitoring controls be implemented:

- who is logged into which work station; how long they are logged in;
- the nature of files that are accessed;
- how long a workstation is idle after an employee logs in;
- irregular patterns in employee logins;
- and manager review of access logs to determine any potential security risks.

State and federal regulations require that security assessments be conducted periodically by the manager of a department with secure data. Depending on the nature of secure documents that the department uses, these assessments might be conducted once a month, but must be conducted at least twice a year. At least once a year, the manager must certify compliance with applicable state and federal security regulations, and must identify areas of security risk as well as improvements in security processes that have been implemented as a result of the security assessment.

5.2 Tips for Selecting Strong Passwords

5.2 Tips for Selecting Strong Passwords

5.2.1 Select a good password

- Use a combination of letters, numbers and special characters ($, *, !, etc.).
- Use the first (or second, or last, ...) letter of each word in a phrase.
- Use upper and lower case characters.
- Choose passwords that are a minimum of eight characters in length.
- Select a password your can remember. For example, use the first (or second, or last, ...) letter of each word in a phrase: "The quick fox jumped over the lazy dog" might yield a password of "Tqfj^1ld"

- Don't use a common word, a friend's name, a pet's name, your nickname, the name of your favorite team, etc. Co-workers, friends, and even casual acquaintances, may know this information.
- Use a different password for each system.

5.2.2 Keep your password secure:

- Change your password when you first receive your computer user-ID.
- Remember to destroy any paperwork that lists the account user-ID and password.
- Change your password when you suspect that someone else may know it. (Keep your password secret!)
- Change your password periodically (every sixty to ninety days).
- Never re-use an old password.
- Never write down a password:
- Do not identify a password as being a password.
- Do not attach the password to a terminal, keyboard, or any part of a computer.
- Never record a password on-line, and never send a password to another person via electronic mail.
- Destroy any paperwork that lists the account user-ID and password.

5.2.3 Don't be a victim of "social engineering"

A frequent cause of loss of password security is "social engineering" - a deliberate attempt by someone to obtain your password through deception. To prevent such loss of your password:

- Never reveal your password to anyone else.
- Help desk personnel, network managers, or computer support personnel should never have occasion to need your password to diagnose problems.
- Don't reveal your password over the telephone, via e-mail, etc.
- Make sure that no one is peering over your shoulder when you type in your password.

5.3 Strong Password Standards

The following standards were established to create and maintain strong passwords. Inclusion of all of the

following in password composition will ensure that your password will be at a low risk for compromise.

5.3.1 Creating a Strong Password

Passwords are required to be a minimum length of 6 characters and should be composed of at least two of the following:

- One UPPERcase or lowercase alphanumeric character;
- One number;
- Or, one Special Character (non-alpha-numeric).

5.3.2 Restrictions

Several types of passwords are considered weak and easy to guess. In order to avoid creating a vulnerable password, the computer system will prevent you from choosing any of the following to create your password:

- Your EUID, account name, or login name;
- Your EagleMail address;
- Any word that can be found in any English or foreign language dictionary;
- Passwords that do not meet minimum length requirements, e.g., h3lp, adm1n, etc.)
- Numerical (digit) substitutions for characters (e.g., pa$$w0rd, etc.);
- Passwords composed of numbers only, i.e.,
- Your social security number,
- Your telephone number,
- Any part of your birth date;
- Blank or null passwords;
- Or, any previously used password.

5.3.3 Security of Your Account and Password

- Passwords for continuing students, faculty, and staff will expire after 120 days from the date on which the password was set.

- Passwords for applicants, transfer students, and returning students will expire 60 days from the date on which their enrollment status changes to a "student" role. This usually occurs when the student registers for classes.
- If you forget your password, or your password expires, go to Account Management System page, http://ams.unt.edu, to reset it.
- Your account has been protected from intruders who attempt to guess your password. After a set number of failed password attempts, your account will be locked in order to prevent further unauthorized access attempts.
- If you attempt to log into your account and your authorization fails as a result of entering invalid passwords, try again in 15 minutes. If you are still unsuccessful, go to the Account Management system page on the web, http://ams.unt.edu, to reset your password.

5.4 Workstation and Computer System Security

You can increase the chances that your computer will not be attacked by an intruder by learning how a computer can become vulnerable to attack. To learn more about the latest types of attacks on computers and how to avoid them, read "How to Secure Your UNT Workstation" found on the information security website: http://www.unt.edu/security. Faculty and staff members should contact their network manager or system administrator for assistance implementing the suggested recommendations. The following information is included in the guide: a description of a typical hacking scene, applying software patches, disabling unnecessary services and servers, the perils of using your computer account with administrative rights enabled, spam ("unsolicited" e-mail), vulnerabilities in commonly used software, peer-to-peer software, why it's good to use password protected screen savers, file and print sharing, and using personal firewalls.

Network managers and system administrators will find the "Code of Good Practices (Reference for Securing Systems)" guide helpful. These best practice documents are available to administrators who would like to learn more about securing windows and unix based systems. The information can be found on the information security website at http://www.unt.edu/security.

5.5 Physical Security

The physical security of computing resources (computers, equipment, files, etc.) is actually the first principle of good security, because as long as someone can obtain physical access to your computer he/she can gain control over it. By instituting a few simple safeguards, you can greatly limit security breaches and other unauthorized access to computing resources. The Texas Property Accounting Standard (§ 403.276) states: "If [an] investigation discloses that a property loss has been sustained by the state through the fault of a state official or employee, the Attorney General shall make written demand on the state official or employee for reimbursement to the state for the loss sustained." In other words, you are held responsible for property that has been assigned to you. This property includes (but is not limited to) computers, pagers, cell phones, etc.

Here are a few helpful hints to safeguard the physical security of items that are your responsibility:

- Log out when leaving your computer.
- Close and lock your office door every time you leave.
- Don't leave your office keys in easily accessible locations-secure them.
- Complete a “Property Custody Receipt” (obtainable from the Asset Management department) to authorize official removal and return of University property from campus
- Restrict the number of keys to your office.
- Know who accesses your office. (It may be necessary to maintain an attendance log for high security areas.)
- Use a screen-saver that requires a password to get back into your computer after the screen saver activates
- Keep your passwords and computer user-ids a secret.
- Report suspicious looking persons or activity to the UNT Police department.
- Express any concerns about physical security to your supervisor.

6 Responsibilities of UNT Faculty, Staff, and Students

6 Responsibilities of UNT Faculty, Staff, and Students

6.1 Special Responsibilities for Faculty

Faculty members should take time to discuss information security with each of the classes. General principles include the following:

- Refrain from sharing computer accounts;
- How to select good passwords;
- Regularly back up their files;
- Purchase virus protection software from the University Bookstore and enable automatic scanning;
- Scan files and disks for viruses or worms before opening; and
- Review the Student Code of Conduct.

Faculty members should also remember to protect student information when posting grades, etc. Researchers should also review "Special Responsibilities for Custodians of Information Resources" found in section 6.2.

6.2 Special Responsibilities for Deans, Department

Heads, Managers and Supervisors

[Excerpt from University Policy 3.10: Computer Use Policy and System Administrator Code of Ethics]

Management should restrict the number of persons granted privileged access to a minimal practicable number, then tell the person who is responsible for overall administration of a system the names of those persons and what functions those persons have been assigned. Persons who are to be given privileged access to a UNT computer system should be selected (or approved) by the Head of the department that owns or manages the operation of the computer system or by another member of management to whom this responsibility has been delegated.

Granting privileged access to UNT computer systems represents an investment of trust. Persons who are to be given such trust by management should be selected carefully, based on personal characteristics of honesty, integrity, and dependable work habits. The manager should clearly define the job responsibilities of each person selected for privileged access to avoid ambiguity over what the privileged user should or should not be doing.

Final responsibility for the security of computer resources rests with the management of the organizations that own or control them. It is the responsibility of management to comply with all computer security standards in force at UNT and to conduct themselves in a manner that will foster security awareness and understanding among users.

- Ensure adequate training opportunities for your staff. Remember, some staff may need more instruction than others, especially when it comes to scanning for viruses, organizing files into directories or folders, backing up files to diskette or tape, etc.
- Document, in the Position Planning Guide/Performance Agreement (UPO-31) any special responsibilities in a position with respect to security. Responsibilities should be commensurate with position's authority.
- Try to carefully assess applicant's trustworthiness before hiring.
- Notify the appropriate system administrators to disable user IDs or other accounts when an employee responsibilities changes or a termination of employment occurs. If the termination could potentially be hostile, the administrator should request that the user ID(s) be disabled immediately.
- If you supervise a system administrator (network/file server manager, other multi-user system manager), review the UNT Information Security Handbook for Faculty, Staff, and Students with that person.

- Promptly report ongoing or serious problems regarding inappropriate computer usage.

6.3 Special Responsibilities for Owners of Information Resources

Most of the administrative information stored on UNT's computing systems is owned by the University. Various administrative units are assigned to control the University's data files that are primarily created and processed within their program areas. For example, the Registrar's Office controls student records; Human Resources manages employee records; and the Controller's Office oversees the University's financial data.

These "owner designees" are responsible for specifying and approving appropriate security controls for the administrative data. Owners of information resources assign custody of UNT's data assets to data custodians (programmers, system administrators, etc.) who implement the controls based on values that they (owners of information resources) have determined. Controls may be specified at various levels (by owners), including:

- whether records may be viewed only, or viewed and updated;
- whether all records may be viewed, or only a portion of all records;
- whether the entire record may be viewed, or only certain fields (such as name, employee id number, euid, birth date, etc.);
- how the information may be accessed

6.4 Special Responsibilities for Custodians of Information Resources (system administrators, data processing managers, resea

The "custodian of an information resource" is the unit charged with the physical possession of certain data or other resources. Custodians are normally technical managers, such as the operators or managers of a multi-user, central or departmental computer system, server, or network of microcomputer workstations. However, persons who maintain internal departmental data about faculty, staff, or students (i.e. personnel information, payroll information, student information, etc.) using departmental resources (databases, spreadsheets, documents, etc.) are also custodians of the information they manage. The end user is the custodian of his or her individual workstation.

Certain designated persons are given broader access to the resources of computer systems because their job responsibilities require such access. Typically, such persons are responsible for providing administrative services on the designated computer(s), services such as system maintenance, data

management, and user support. The term "broader access" covers a range -- from wider access than given to an ordinary system user, up to and including complete access to all resources on the computer system.

Responsibilities include:

- Control physical and login access to University computer resources under its possession. Security controls for these resources shall take into account local, state and federal reporting and auditing requirements, as well as provisions to eliminate, as far as is feasible, the incidence of theft, fraud, destruction, or other abuses of University computer resources.

- Take appropriate measures to protect the data from loss due to natural disaster, hardware failure, user error, and system contamination (e.g. computer virus) or other malicious activities. The custodian should archive the data located on the University computer system in accordance with operational and data archival procedures.

- Ensure that, if possible, the process by which a user accesses the resources of their computer resources of their installation displays a message regarding a user's responsibility to comply with the provisions of this policy.

- Enforce compliance with provisions of software licensing agreements and other computer resource contracts for the computer installation. Reasonable steps should be taken to not permit unauthorized copies of computer software and manuals to be obtained.

- Report security problems to the Office of the Associate Vice President for Computing and Communications Services.

Persons given broader-than-normal access privileges on UNT computer systems agree:

- Not to "browse" through the computer information of system users while using the powers of privileged access unless such browsing: is a specific part of their job description (e.g., an auditor); is required during file system repair, management, or restoration; is necessary to investigate suspicious or system-impairing behavior; or is specifically requested by, or has the approval of, the person who authorized their privileged access. Browsing should never be done unless it is in the best interest of UNT.

- Not to disclose, to any unauthorized person, computer information observed while operating with privileged access.

- Not to copy any computer information for any purpose other than those authorized under their defined job responsibilities.

- Not to intentionally or recklessly damage or destroy any UNT computing resources.

- Not to accept favors or gifts from any user or other person potentially interested in gaining access to UNT computer systems.

- Not to do any special favors for any user, member of management, friend, or any other person regarding access to UNT computers. Such a favor would be anything that circumvents prevailing security protections or standards.

- Not to tell or disclose to any unauthorized person the information required to gain privileged access, or to engage in careless practices that would reveal that information to unauthorized persons.
- Not to attempt to gain or use privileged access outside of assigned responsibility (e.g., on other machines) or beyond the time when such access is no longer required in assigned job functions.
- Not to change or develop any computer software in a way that would (a) disclose computer information to persons not authorized to have it, or (b) make it possible to retain any special access privilege once that authorized privilege has been terminated by management.
- Not to make arrangements on computer system(s) under their charge that will impair the security of other systems. In order to comply with this restriction, a system administrator setting up authorized networking connections should make use of available controls and protections as fully as reasonably possible.
- Report all suspicious requests, incidents, and situations regarding a UNT computer to an appropriate member of local management, Internal Audit, UNT Police, and/or to UNT FIRST (Forum for Incident Response and Security Teams).
- Use all available software protections to safeguard computer system(s) under their charge from unauthorized access by any person or another computer.
- Take steps to the best of their ability to comply with all computer security standards and policies in force at UNT and furthermore, advise management and/or designated computer security representatives at UNT of deficiencies in these standards.
- Conduct themselves in a manner that will foster security awareness and understanding among users.

6.5 Special Responsibilities for the Information Security Coordinator

The information security coordinator is responsible for managing the University information security program. Responsibilities include the following:

- Ensure that adequate security procedures, including backup, disaster recovery, and contingency planning, have been formulated for the centrally administered computer systems.
- Coordinate the implementation of security procedures, including backup, disaster recovery, and contingency planning, for the departmental computer systems and personal computers.
- Establish mechanisms for monitoring compliance with and violations of University computer resource security policies and standards.
- Establish procedures for investigation, logging, and management reporting and follow-up of access

violations.

- Perform periodic risk assessments and security audits of existing and proposed systems.
- Oversee the development and maintenance of a comprehensive Computer Resource Security Policy Manual to include security procedures to implement University computer resource security policies and standards.
- Oversee the development of training courses for training employees in University computer resource security policies, standards, and procedures.
- Gather information from the Information Resource Custodians and report as necessary and appropriate.

6.6 Special Responsibilities for Students

Many computing services are available to UNT students, including:

- Use of General Access Labs
- Web-based enrollment services (admission, registration, financial aid, student accounting);
- Student e-mail services (Eaglemail)
- Web page publishing
- Web-based course instruction (WebCT)
- Assistance from Help Desk personnel

Use of these services is a privilege granted to the members of the University community. In turn, users agree to abide by the applicable policies of the University, as well as federal, state and local laws. Here are some general guidelines to help students comply with these policies and laws, and to keep these valuable resources functioning and available to all who need them:

- Be aware of the thousands of others who depend on the University's computer systems, network, and the Internet to do their work. Consider how your computer behavior will affect them and chose what you know is right.
- Understand that University policies address academic dishonesty, including theft, disruptive conduct, and misuse of materials and property. These policies apply to computing activities as well as activities in the classroom, residence halls, or elsewhere on campus.
- Don't copy software unless specifically authorized.
- Don't allow other students, relatives, or any other person to use your computer account(s). You will be held accountable for any abuse of computing resources by persons you allow to use your

account.

- Protect your password -- keep it secret and change it regularly. Choose your password wisely. Be aware that the University has had incidents of students stealing other students' passwords for the purposes of performing prohibited acts.

- Understand what you are authorized to do. Know that your computer accounts are provided so you can send and receive mail, read and post notices to new groups, and access library and other information resources. General Access Lab computers, networks, and printers are available to you so that you can do word processing, make spreadsheets, and access central University computers and the Internet. In some cases, your professors will authorize access to additional resources so that you can do class assignments. You can use UNT's computers as long as your activities add no additional cost to UNT and as long as you continue to obey the policies and laws. In general, you can not use UNT's computers for commercial purposes. (One exception, it's okay to advertise personal items for sale within the "unt.forsale" newsgroup.)

- Understand that the privacy of messages you receive and files you create is limited. Although your use of University computers is not generally monitored, there may be circumstances (hardware failure, hacker attacks, etc.) in which computer system administrators may need to look at information and files to solve problems and protect systems. (System administrators should treat any information they might see that turns out to be unrelated to the problem as strictly confidential.)

- Comply with reasonable requests and instructions from the computer system operator/administrator. (A system operator/administrator should NEVER ask for your password. If a request seems unreasonable, verify the identity of the person claiming to be a system operator or administrator.)

- Don't "hack" (disrupt computers systems and networks, send forged electronic messages, invade the privacy of others, steal other people's passwords, etc.).

- Report security problems immediately to your instructor, system administrator, or other appropriate University authority.

6.7 Special Access for Auditors

[Excerpt from University Policy 3.10: Computer Use Policy]

There will be occasions when auditors require access to University computer resources and data files. The access will be permitted in accordance with these guidelines.

Internal Auditors from the University of North Texas:

- Shall be allowed access to all University activities, records, property, and employees in the performance of their duties.

- Shall notify the Office of the Associate Vice President for Computing and Communications Services and the Office of the Vice President for Legal Affairs and General Counsel prior to

accessing individual data files.

State and Federal Auditors:

- Will be granted access to University computer resources and data files on an as needed basis, as approved by the Office of the Vice Chancellor and General Counsel.

6.8 Large Group E-Mail Guidelines

The Provost and all Vice Presidents recommend the following guidelines for using large E-mail groups:

- Departments and individuals should be judicious in sending E-mail to all faculty and staff. Many recipients may consider the message to be annoying "junk mail," especially if "everyone" messages continue to proliferate at the current rate. As a general guideline, the message should be of sufficient general value that it would justify being sent as a memorandum if E-mail were not available. In other words, is the message important enough to justify sending to virtually every University employee? Campus-wide discussions should use Usenet news groups, not E-mail.
- All large group mailings should use appropriate mail groups. A public group will be maintained in the GroupWise (GW) address directory that will include all UNT faculty and staff in the GW directory, as well as more limited groups such as department heads and account holders. Offices or individuals that make frequent or regular large group mailings that are not official notifications to all faculty and staff are encouraged to maintain their own groups. Messages to these groups should have an introduction indicating willingness to remove an individual from the group if requested by return E-mail.
- Anyone sending mail to large groups should use the GroupWise send options to conserve system resources.

6.9 General Responsibilities for All Users

- Know the Basics of Information Security
- Learn about possible Security Problems
- Review and comply with the UNT Computing Policies and Guidelines
- Review State and Federal laws governing computing standards and crimes.
- Follow procedures for Acceptance of Computing Policies and Procedures.
- Report security incidents immediately.
- Use the University computer resources responsibly, respecting the needs of other computer users.

7 Acceptance of Security Policies & Procedures

The UNT Information Security Handbook for Faculty, Staff, and Students is published in partial fulfillment of the requirements of Texas Administrative Code §202.77, Information Security Standards: All authorized users (including, but not limited to, institution of higher education personnel, temporary employees, and employees of independent contractors) of the institution of higher education's information resources, shall formally acknowledge that they will comply with the security policies and procedures of the institution of higher education or they shall not be granted access to information resources. The institution of higher education head or his or her designated representative will determine the method of acknowledgement and how often this acknowledgement must be re-executed by the user to maintain access to institution of higher education information resources.

This handbook is available on the information security website at http://www.unt.edu/security. It contains links to relevant policies and procedures, and is updated as needed by information security personnel. All official University computing policies should be available in the University policy manual, volume 2, section 3, http:/www.unt.edu/policy.

Use of any university computing resource services as acceptance of UNT's computing and security polices and practices. Faculty, staff, and students agree to abide by the policies and procedures that govern the use of the University's automated information systems, and will accept the responsibility to protect information as described within the Family Education Rights and Privacy Act, the Texas Public Information Act, security policies and procedures of UNT as well as other applicable federal and state laws. Training opportunities should be taken advantage of as necessary in order to fully understand and fulfill these responsibilities.

8 Incidents and Emergency Response

Security violations, suspected or confirmed, should be reported right away. UNT faculty, staff, and students can report problems in several ways.

- Contact the Information Security Team (e-mail security@unt.edu or call 369-7800);
- Contact your department network manager/distributed support;
- Send e-mail to first@unt.edu ;
- Notify your supervisor;
- Call the Computing and Information Technology Center Helpdesk, 565-2324, and ask the consultant for assistance with a security problem;
- Or, contact the UNT Police Department, 565-3000, if criminal activity is suspected.

8.1 Information needed by the security contact

In the event that you need to report a security incident, the following information will be needed:

- your name, department, telephone number, e-mail address, etc.;
- the name of the person who discovered the incident/crime and their contact information;
- a description of what happened;
- the date and time of the incident;
- the location where the incident occurred (department, building/room number);
- the names of individuals involved in incident (if known);
- the names of witnesses (if known);
- and documentation, or logs, of the incident (if available).

9 Sanctions

Violations of University policies and applicable state or federal laws are cited in University policies, handbooks, or other guides. A brief description of sanctions can be found below. This list is not intended to usurp other disciplinary or legal measures associated with violations of policy or law.

Penalties for violations of University policy range from loss of computer resource usage privileges to dismissal from the University; and, may also include prosecution, and/or civil action. Referrals for legal action will be made through the Office of the General Counsel.

- If the offender is a faculty member, his or her supervisor (usually the department chair) shall initially recommend to the dean and thereafter to the Provost the appropriate sanction. When termination is recommended, the faculty member may appeal to the University Review Committee or to the University Tenure Committee, whichever is appropriate per the University of North Texas Faculty Handbook.
- If the offender is a staff member, the procedures to be followed are those specified in the "Discipline and Discharge Policy" of the University of North Texas Personnel Policy Manual.
- If the offender is a student, the procedures to be followed are those specified in the "Code of Student Conduct and Discipline" as printed in the University of North Texas Student Handbook. If the student in violation of this policy is also an employee of the University, sanctions may include termination of employment.
- Other State and Federal Laws may be applicable.

10 UNT Computing Policies, Guidelines, and

Handbooks

10 UNT Computing Policies, Guidelines, and Handbooks

10.1 Computing Policies

- UNT Policy 3.1 Computing and Information Technology Center General Policies:

http://www.unt.edu/policy/UNT_Policy/volume2/3_1.html

- UNT Policy 3.6 Information Resources Security Policy:

http://www.unt.edu/policy/UNT_Policy/volume2/3_6.html

- UNT Policy 3.9 Web Publishing Policy:

http://www.unt.edu/policy/UNT_Policy/volume2/3_9.html

- UNT Policy 3.10 Computer Use Policy:

http://www.unt.edu/policy/UNT_Policy/volume2/3_10.html

- UNT Policy 3.11 Network Connections Policy:

http://www.unt.edu/policy/UNT_Policy/volume2/3_11.html

- UNT Policy 18.5.7 Student E-Mail Policy:

http://www.unt.edu/policy/UNT_Policy/volume3/18_5_7.html

- UNT Internet Account Policies:

http://www.unt.edu/ACSUNIX/policies/general.html#internet

- Academic Computing Services UNIX Host System Policies:

http://www.unt.edu/ACSUNIX/policies/general.html#host

10.2 Computing Guidelines

- How to Secure Your UNT Workstation:

http://www.unt.edu/security/awareness/userguide.html

- Large Group E-Mail Guidelines:

http://www.unt.edu/irc/policy/EveryoneMessageGuidelines.htm

- System Administrator Code of Ethics:

http://www.unt.edu/ccadmin/security/SecurityManualUpdate/saethics.htm

- Desktop Applications Software Guidelines:

http://www.unt.edu/irc/policy/deskapps.htm

- Web Publishing Guidelines:

http://www.unt.edu/irc/webgdlnsv2.htm

10.3 Handbooks and the University Policy Manual

- Faculty Handbook:

http://www.unt.edu/vpaa_fy0203_fhb/homepg.html

- Staff Information:

http://www.unt.edu/hr

- Employee Handbook:

http://www.unt.edu/hr (see "Resources/Publications")

- Code of Student Conduct:

http://www.unt.edu/ACSUNIX/policies/general.html#host

- University Policy Manual:

http://www.unt.edu/policy

11 State and Federal Laws

- Information Security Standards -Texas Administrative Code Part Title 1, Chapter 10, Section 202:

http://info.sos.state.tx.us

- Computer Crimes- Texas Penal Code, Chapter 33:

http://www.capitol.state.tx.us/statutes/petoc.html

- Telecommunications Crimes- Texas Penal Code, Chapter 33(a):

http://www.capitol.state.tx.us/statutes/petoc.html

- Tampering with a Governmental Record- Texas Penal Code, Chapter 37:

http://www.capitol.state.tx.us/statutes/petoc.html

- Computer Fraud and Abuse Act of 1986- U.S. Penal Code, Title 18, Section 1030:

http://www.capitol.state.tx.us/statutes/petoc.html

- Fraud and related activity in connection with computers- U. S. Penal Code, Title 18, Chapter 47:

http://www.capitol.state.tx.us/statutes/petoc.html

- Fraud and False Statements, Section 1030:

http://www.usdoj.gov/criminal/cybercrime/Patriot_redline.htm

- Federal Copyright Law:

http://www.copyright.gov/title17

- Digital Millennium Copyright Act:

http://www.copyright.gov/legislation/dmca.pdf

- Computer Software Rental Amendments Act of 1990:

http://www.copyright.gov/reports/software_ren.html

- Texas Open Records Act:

http://www.oag.state.tx.us/opinopen/og_faqs.shtml

http://www.co.denton.tx.us/OpenRecords

- FERPA (Family Educational Rights and Privacy Act):

http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

- HIPPA (Health Insurance Portability and Accountability Act):

http://www.dol.gov/ebsa/newsroom/fshipaa.html

- GLBA (Gramm-Leach-Bliley Act):

http://www.ftc.gov/privacy/glbact

12 UNT Computing Resources and Supportv

- UNT Computing and Information Technology Center (CITC):

http://www.unt.edu/ccadmin

- UNT CITC Helpdesk:

http://www.unt.edu/helpdesk

- Information Security Team:

http://www.unt.edu/security

- Virus Information and Procedures:

http://www.unt.edu/virus

- Distributed Computing Support and Management Team:

http://www.unt.edu/dcsmt

- UNT Network Managers:

http://www.unt.edu/helpdesk/netmanDepartments.htm

- General Access Computer Labs:

http://www.gal.unt.edu/

- UNT Police Department:

http://www.unt.edu/police

13 Computer Security Terminology

Access- to approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of information resources.

Access Control- the enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

Availability- ability to be present or make ready for immediate use

Breach or Incident- an event which results in unauthorized access, loss, disclosure, modification, or destruction of information resources whether accidental or deliberate

Computer- an electronic, magnetic, optical, electromechanical, or other high-speed data processing device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device.

Computer Security- those measures, procedures, or controls which provide an acceptable degree of safety of information resources from accidental or intentional disclosure.

Confidential Information- information that is excepted from disclosure requirements under the provisions of the Texas Public Information Act or other applicable state or federal law.

Contingency- intended for use in circumstances not completely foreseen.

Control- a protective action, device, policy, procedure, technique, or other measure that reduces exposure.

Critical Information- information that is defined by the agency to be essential to the agency's function(s).

Custodian of an Information Resource- a person responsible for implementing owner-defined controls and access to an information resource.

Data- a representation of facts or concepts in an organized manner in order that it may be stored, communicated, interpreted, or processed by automated means. Data includes all files, regardless of size or storage media, including e-mail messages, system logs, and software (commercial or locally developed).

Data Security- those measures, procedures, or controls which provide an acceptable degree of safety of information resources from accidental or intentional disclosure.

Department Head - An employee of the university with budgetary authority over users of an information resource.

Disaster- a condition in which an information resource is unavailable, as a result of a natural or man-made occurrence, that is of sufficient duration to cause significant disruption in the accomplishment of agency program objectives, as determined by agency management.

Disclosure- unauthorized access to confidential or sensitive information.

Hacker- a person who illegally gains access to and sometimes tampers with information in a computer system

Harm- includes partial or total alteration, damage, or erasure of stored data, interruption of computer services, introduction of a computer virus, or any other loss, disadvantage, or injury that might reasonably be suffered as a result of the actor's conduct.

Incident or Breach- an event which results in unauthorized access, loss, disclosure, modification, or destruction of information resources whether accidental or deliberate

Information- that which is extracted from a compilation of data in response to a specific need.

Information Resource- the procedures, equipment, facilities, software and data which are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

Integrity- the state that exists when computerized information is predictably related to its source and has been subjected to only those processes which have been authorized by the appropriate personnel.

Owner of an Information Resource- a person responsible for a business function and for implementing controls and access to information resources supporting that business function.

Password- a protected word or string of characters which serves as authentication of a person's identity (personal password), or which may be used to grant or deny access to private or shared data (access password).

Risk- the likelihood or probability that a loss of information resources or breach of security will occur.

Security Controls- hardware, programs, procedures, policies, and physical safeguards which are put in place to assure the integrity and protection of information and the means of protecting it.

Sensitive Information- information maintained by state agencies that requires special precautions to protect it from unauthorized modification or deletion. Sensitive information may be either public or confidential. It is information that requires higher than normal assurance of accuracy and completeness. The controlling factor for sensitive information is that of integrity.

User of an Information Resource- an individual or automated application authorized to access an information resource in accordance with the owner-defined controls and access rules.

Virus- an unwanted computer program or other set of instructions inserted into a computer's memory, operating system, or program that is specifically constructed with the ability to replicate itself or to affect the other programs or files in the computer by attaching a copy of the unwanted program or other set of instructions to one or more computer programs or files.

Worm- A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down