UNT | SYSTEM
IT Shared Services

University of North Texas System (UNTS)

Information Security Users Guide

The Information Security Users Guide contains computing guidelines and policy for faculty, staff and students of the University of North Texas System, which is comprised of the campuses of the University of North Texas, UNT Health Science Center, UNT Dallas, and the services that support them. The practices and standards found within are based on the requirements of the Texas Administrative Code §202.70-78 and the International Organization for Standardization's ISO 27001 and ISO 27002 frameworks which have been adopted by the University of North Texas System. This document is available for online review and printing. It is required reading for anyone using the UNT System institutions' computing resources. Departments that work with financial, medical, academic, or other sensitive information are required to read the Information Security Users Guide and become familiar with the policies and guidelines listed within. This is a continued effort by The University of North Texas System to prevent FERPA, HIPAA, GLBA, DMCA, Texas Identify Theft Enforcement and Protection Act, Texas Medical Records Privacy Act, Payment Card Industry Data Security Standards, Digital Millennium Copyright Act, and Copyright Law infringement.

Table of Contents

Part I – Information Security Standards for All Users

1 Purpose

The purpose of this Users Guide is to help managers and users of information resources gain an understanding of the basic knowledge necessary to protect these resources. Information resources are the physical and logical data information assets of the university. Gaining knowledge about how to protect these resources can ensure that intrusion, alternation, or loss will be less damaging. This Users Guide should also be considered a guide for learning best practices for securing information resources. It is a guide to help protect against security breaches, improper access to computing resources, unauthorized disclosure of information, and internal and external threats. The responsibilities of university faculty, staff, and students are presented, as well as the services provided by the Information Security staff. Also included, are links to UNT System (UNTS) computing policies, guidelines, and standards, as well as links to state and federal laws to provide a basis for the standards that governed the development of the Users Guide.

2 Scope

The UNTS institutions depend upon their computer systems and networks in all aspects of their missions, from scheduling classes and registering students to generating employee paychecks. The continued operation of information systems depends upon appropriate levels of information security. Maintaining security requires all employees to do their part.

The security of information must be maintained through hardware and software controls. Additionally the behavior of users of the computer hardware, software, and information affects the confidentiality, integrity, and availability of that information. This document gives the information resource user the basic knowledge needed to protect institutional information and assets from misuse, abuse, unauthorized access or unauthorized disclosure. Institutionally owned assets include the hardware (workstations, servers, etc.) software (operating systems, desktop software, etc.) and information that the hardware and software allow access. Such information may be sensitive or confidential and may have policies or laws that protect its availability, integrity, and confidentiality.

3 Information 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 that results in unauthorized access, loss, disclosure, modification, or destruction of information resources whether accidental or deliberate

CERT – Computer Emergency Response Team; lead by a member of the ITSS Information Security team and may consists of members of any affected department's staff

Confidential Information - information that is accepted 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)

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

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

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

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

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

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

Password - a combination of characters and numbers which serve as authentication for a user's identity

Phishing - an attempt to obtain sensitive information by using one or more types of counterfeit media usually through email

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

Secure Socket Layer (SSL) – a secure protocol used for encrypting messages sent over the internet.

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

Sensitive Information - information classified by state agencies that requires special precautions to protect it from unauthorized modification or deletion

Social Engineering - a deliberate attempt by someone to obtain sensitive information through deception

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

VPN – a virtual private network is a secure tunnel over the internet that can be used to access remote services

4 The Basics of Information Security

4.1 Maintaining Confidentiality of Information

4.1.1 Confidentiality and Open (Public) Records

Most types of institutionally owned information (records) are defined as either "Confidential" or "Public." Information that is classified as confidential cannot be disclosed or disseminated to the public (people who aren't employees of the institution 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

Everyone has a responsibility to protect information about students from public disclosure, no matter where the information resides. 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. FERPA requires written consent be obtained by the student before disclosing the student's education records containing personally identifying information. Exceptions to requiring consent are made in limited circumstances, such as when needed by local emergency responders during a health or safety emergency. More information about FERPA is found later in this document in section 15.1.

4.1.3 Protecting Open Directory Information

The following items are considered open directory information for students:

- Student's name
- Address
- E-mail address
- University assigned Enterprise User Identification Number (EUID) so long as the EUID cannot be used to gain access to the student's education records except when used in conjunction with another factor to authenticate the student's identity.
- Date and place of birth
- 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)

Students can request for their directory information to be withheld. The students who have requested information to be withheld are identified within the Enterprise Information System (EIS). All employees of a UNT System institution who regularly deal with student information should attend FERPA training, available through the Registrar's Office at each institution. Open directory information includes general information (as listed above) but it is important that all other student information be kept confidential. Please contact the Registrar's Office of your institution for additional information.

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) allows the disclosure of Texas state agencies employee records including public institutions. This information includes, but is not limited to:

- Employee name
- Sex
- Ethnicity
- Salary
- Dates of employment
- Title
- Home and mailing addresses
- Home phone numbers

Employees may restrict disclosure of their home address, mailing address, personal phone numbers, emergency contact information, or information about family members. Employers are required to ask each employee their preference upon hire. Requests for information from the public should be referred to the Office of General Counsel.

4.1.5 Ensuring confidentiality of information

- Identify confidential information as "CONFIDENTIAL" on printouts, disk, screen, or anywhere that it is stored or displayed.
- Choose good passwords, and keep them secret. Passwords are confidential, too.
- Logout and/or lock the office when you're away from your desk.
- Don't permit another person to use your account.

- Use special care when posting grades (assign random numbers rather than using parts of social security numbers).
- Secure printouts and other documents. Retrieve your printouts as soon as possible. Keep confidential or sensitive documents out of plain view.
- Shred CONFIDENTIAL documents or place in locked paper recycling bins. Make sure discarded disks and tapes are unreadable.
- Attend security awareness and FERPA training and send your student workers, too.

4.2 Maintaining the Integrity of Information

Information needs to be accurate and complete to be useful. Records and documents must be protected from unauthorized modification or destruction. Here are steps to take to keep the integrity of information intact:

- Check your work for accuracy and completeness.
- Choose good passwords, and keep them secret.
- Logout and/or lock the office when you're away from your desk.
- Don't permit another person to use your account.
- Use the VPN (Virtual Private Network) when remotely accessing secure resources.
- Use virus detection/protection software.
- Use encryption when transmitting sensitive data over the web (See Section 5.2 Protecting Sensitive Data).
- Make sure you have backups of important information (on paper, disks, tape, or file server).
- Control who has access to the data that you manage and what kind of access they have.
- Check references when hiring.

4.3 Ensuring the Availability of Information

4.3.1 Preparing for a Disaster or Loss of Services

Disasters can strike at any given moment. Adequate plans must be in place to address how every department would operate in the event of either a natural or technological disaster that could potentially cause an outage to UNT System enterprise services. It is important to have a plan in place that addresses how critical operations would continue to operate if enterprise services became unavailable. The plan should provide for both short and extended periods of a services' outage. Contingency plans are made up of procedures and lists. Procedures should address how to accomplish basic tasks without computers and networks.

Plans should include the following:

- 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.
- Critical data, hardware, and software critical documentation.
- Critical supplies and resources (computers, telephones, monitors, network access, etc.), 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.).
- Storage location of critical backup data.
- Date of the last review of all elements of the contingency plan.

A contingency plan is a living document. Some of the information changes frequently and should be updated and disseminated. Departments should test their plans periodically to ensure the contingency procedures are still applicable.

4.3.2 Backing up Files

In the event of a disaster, it is possible that files on your workstation may become unavailable. Any file critical to daily operations should always be backed up to a secure location.

The following guidelines should be followed to ensure the availability of your data:

- Add backing up files to your weekly or monthly to-do list.
- Know how often the files on your department's file server are backed up.
- Back up what you can't replace.
- Back up or archive your important e-mail messages.
- Keep a backup in a secure location other than your office.
- Keep your files organized to simplify backups.
- Use version numbers in filenames and keep several recent versions.
- Make sure your IT manager approves your backup location.

If you need assistance, contact the IT manager in your department.

4.3.3 Mitigating a Disaster

Disasters cannot always be prevented, but following the steps below can help reduce the impact to institutional data:

- 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 at least once a week.
- Ensure the physical security of your office 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 user account.
- Use antivirus software.

5 Information Safeguards

5.1 Definition of Sensitive Data

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. UNT institutions utilize classification standards to determine the sensitivity of data. Sensitive data is any information that falls into category I or II as seen below. Data classified as categories I or II may require additional security controls.

Category I: Category I includes confidential information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g. the Texas Public Information Act), or information that requires a high degree of security. Examples include social security numbers, credit card numbers, protected health information, student information, and in some cases student directory information

Category II: Category II includes information that is proprietary to the institution or has moderate protection requirements. Examples include departmental information, non-confidential information.

Category III: Category III information includes all other types of information that have little or no protection requirements, or information intended for public release as described in the Texas Public Information Act.

5.2 Protecting Sensitive Data

The State of Texas information security standards require encryption of sensitive data in certain instances. To find out what specific options are available to encrypt sensitive data, contact your department IT Manager.

5.2.1 Encryption in Transit

In order to ensure the integrity of sensitive data, it is important to transmit data securely. Data classified as category I is required to be encrypted while in transit. It is

also recommended that data classified as category II be transmitted securely when possible. Examples of ways to encrypt transmitted messages are encrypted instant messaging, Secure Socket Layer (SSL) enabled web forms (https://), and Virtual Private Network (VPN) access.

5.2.2 Encryption at Rest

Sensitive data should also be encrypted while it is being stored. Using strong encryption will greatly reduce the damage incurred by a compromise and can even eliminate the chances of information disclosure. Data classified as category I is required to be encrypted at rest, and it is also recommended that category II data be encrypted at rest as well. Examples of where encryption at rest might be used are encrypting files and folders, encrypting database tables or columns, or encrypting disks.

5.2.3 Compensating Controls

In some cases it may not be practical to utilize encryption to protect sensitive data. In these rare cases, it is required to document and implement compensating controls, and seek an exemption from this requirement from your institutional information security officer. Compensating controls are a combination of practices and technology that can be implemented to lessen the risk of sensitive data disclosure.

In addition to the encryption requirements, data classified as categories I or II should be protected using the following measures:

- 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 workstation on which secure documents are accessible.
- Follow strong password standards (See Section 5.3.1 Creating Strong Passwords).

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

- 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.

- A review of access logs of a computing resource to determine any potential security risks.

OneDrive for Business may be used to store files for UNT System institutions' business purposes only. Because OneDrive for Business automatically stores files in two locations (on the computing device and also in OneDrive), care must be taken to ensure that information is stored in a manner that ensures compliance with information security policies. Confidential information may not be stored on mobile computing devices, i.e., laptops, tablets, etc., unless the device is encrypted. Personally-owned information and files may not be stored in OneDrive.

For further information about encryption and other topics on information security, please see the UNT System Information Security Handbook. See section 12.4 for information about encryption.

5.3 Passwords

5.3.1 Creating Strong Passwords

The following guidelines are suggestions that will help create strong passwords and reduce the risk of your password being compromised:

- Use a combination of letters, numbers and special characters ($, *, !, etc.).
- Use the first letter of each word in a phrase.
- Use upper and lower case characters.
- Choose passwords that are a minimum of eight characters in length.
- Use a different password for each system.

The following should be avoided when creating new passwords:

- Using common words, a friend's name, a pet's name, the name of your favorite team, etc.
- Using your EUID (Enterprise User ID).
- Using your birthdate, social security number, phone number, or other personally identifiable information.

5.3.2 Securing Your Password

After a set number of failed password attempts, your institutional 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 UNT website to reset your password.

Other ways to keep your password secure:

- Remember to destroy any paperwork that may display your EUID (Enterprise User ID), enterprise password, or employee id.
- Change your password when you suspect that someone else may know it.
- Change your password periodically (every sixty to ninety days). Never re-use an old password.
- Never write down a password.
- Never send a password to another person under any circumstance, not even your computing support staff.
- Passwords will expire 1 year from the date on which the password was set.
- If you forget your password, or your password expires, go to the Account Management System page to reset it.
- Never use the same password for more than one system.

5.4 Securing Systems and Workstations

All workstations should employ antivirus software for protection against malicious code. ITSS Information Security has a site license for McAfee Antivirus software that can be downloaded from the ITSS Information Security antivirus webpage with a valid EUID and password. The antivirus software should be configured for regular updates and automatic scans to remain effective. In addition, you can reduce your risk of compromise by following these practices:

- Verify the contents of unexpected email attachments or instant messenger links before opening them.
- Utilize a firewall.
- Apply current patches to your operating system.
- Keep all software up to date by applying current patches. Examples include browsers, browser add-ins such as java and flash, and popular office productivity products.

5.4.1 Secure Remote Access

In order to ensure the security of institutional computing systems, it is a necessity to utilize the UNT Virtual Private Network (VPN) when accessing resources from off campus. The UNT VPN provides a secure connection to UNT System networked resources. The following pre-requisites must be met in order to access resources via the UNT VPN:

- A reliable internet connection – It is highly recommended to have a high speed internet connection available when accessing resources remotely.
- Up to date software – Any computer being used to access institutional resources must have up to date operating system security patches and antivirus software.

- Prior Approval – Before accessing resources remotely, information resource users must obtain approval from their supervisor.

Once the above pre-requisites have been met, users may login to the VPN at https://vpn.unt.edu.

For additional help with using the VPN, contact your department IT support staff or help desk.

5.4.2 Preventing Social Engineering & Phishing

Social engineering is a deliberate attempt by someone to obtain sensitive information through deception. Phishing is an attempt to obtain sensitive information by using one or more types of counterfeit media. To prevent loss of your password or other sensitive data:

- Never reveal your password to anyone. This includes your computer support personnel.
- Shred documents containing sensitive data.
- Do not open suspicious email. Be aware of emails containing misspellings, awkward phrasing, and questionable links.
- Confirm the identity of an individual before divulging potentially sensitive information.

5.5 Ensuring Physical Security

The physical security of computing resources is a key principle of security. If someone can obtain physical access to a computer, he or 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 that you are to be held responsible for property that has been assigned to you. This property includes (but is not limited to) workstations, cell phones, and any other type of electronic device.
Here are some ways to safeguard the physical security of computing resources:

- Logout when leaving your computer.
- Close and lock your office door every time you leave.
- Don't leave your office keys in easily accessible locations.
- Ensure that you are authorized to take institutionally owned property offsite.
- 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 account names a secret.
- Report suspicious looking persons or activity to campus police.
- Express any concerns about physical security to your supervisor.

6 Information Security Roles and Responsibilities

6.1 Responsibilities for Information Resource Users

Information resource users are individuals authorized to use institutional computing resources, including faculty, staff, and students. All users are required to comply with all institutional computing policies. They are responsible for the accounts assigned to them and will be held accountable for any activity within the account, including the actions of any automated processes running on their behalf. Users may only use accounts assigned to them to access institutionally-owned information resources.

Individuals given special privileged access to a computing resource must maintain the confidentiality, integrity, and availability of that resource at all times.

For example:

- Users may only browse or copy information obtained through privileged access as required by their job.
- Users should ensure that data is not altered or destroyed through the use of their privileged access.

Users inappropriately using computing resources are subject to disciplinary procedures under the appropriate institutional policy, as well as federal or state law.

6.2 Responsibilities for Supervisors

Supervisors are responsible for requesting and maintaining proper access for their employees as the employee's status changes. Supervisors should only request the minimum access to information resources that is necessary for an employee's job function.

6.3 Responsibilities for Information Resource Owners

Information Resource Owners are individuals assigned to control one or more information resource. For example, the Registrar's Office controls student records; Human Resources manages employee records; and the Comptroller's Office oversees the institutions' financial data.

Information Resource Owners are responsible for specifying and approving appropriate security controls for the information resource. Owners of information resources assign custody of institutional data assets to data custodians, such as programmers or system administrators who implement controls based on values that owners of information

resources have determined. Controls may be specified at various levels, as to how the information may be accessed.

In the event that information resources are used by more than one major business function, information resource owners must reach a consensus and assign a designated information resource owner. The designated information resource owner will be the proxy for the other information owners, coordinate the control requirements, and inform custodians and users of all applicable requirements, agreements, and policies.

6.4 Responsibilities for Custodians of Information Resources

Custodians are individuals charged with the physical possession as well as the technical and procedural safeguards of a computing resource. It is important to note that each individual user is the custodian of his or her workstation. Custodians are required to implement and maintain both physical and technical safeguards that meet the requirements established by the information resource owner(s), as well as those of ITSS Information Security.

6.5 Responsibilities for Vendors and Persons of Interest

Any non-university affiliated individual requesting access to UNT institutional computing resources is responsible for following all institutional computing policies and standards. Written agreements are required before access is granted to an individual for a UNTS owned information resource. It should also be noted that the faculty or staff member sponsoring this individual is ultimately responsible for ensuring compliance. They are also required to ensure that appropriate non-disclosure agreements are in place, and to notify information resource owners and custodians when access is no longer needed.

7 Acceptance of Security Policies & Procedures

All information resource users must formally acknowledge compliance with all UNT System institutional computing policies and procedures before gaining access to systems. Compliance is required throughout an employee's tenure, beginning with the New Employee Onboarding process facilitated by Human Resources. Supervisors are responsible for ensuring that their staff meets this requirement.

8 Security Training and Awareness

Security Awareness training is required for all new employees and is to be conducted as a part of the onboarding process. Training is also required annually for employees that deal with sensitive data. Annual training is strongly recommended for any employee with access to information resources.

Information about and links to the online information security awareness training can

be accessed from the ITSS Information Security training page.

9 Responding to Security Incidents

Security violations, suspected or confirmed, should be reported immediately. Faculty, staff, and students of UNT institutions can report problems in several ways.

Students should report any problems directly to their campus helpdesk.

- UNT Denton – (940) 565-2324
- UNT HSC – (817) 735-2192
- UNT Dallas – (972) 780-3626

Faculty and staff should notify their supervisor and report the problem to their computer support staff.

If criminal activity is suspected, contact the campus police.

- UNT Denton – (940) 565-3000
- UNT HSC – (817) 735-2210
- UNT Dallas – (972) 780-3009

When reporting a security incident you may need to provide the following information:

- Your name, department, telephone number, and e-mail address.
- The name of the person who discovered the incident and their contact information.
- A detailed description of the incident, including the date and time
- The names of any other individuals involved in the incident.

Part II: Information Security Standards for Technical Users

10 Server Configurations

Microsoft Windows servers should be configured in the following fashion as a baseline configuration:

- Disable the guest account.
- Remove or disable any unnecessary services and applications.
- All machines should have an anti-virus program and a firewall enabled.
- Audit the system at least once per week.
- All machines connecting to the network should have the latest software installed, firewall enabled, and an anti-virus program installed.
- Hosts should automatically disable accounts for a period of time after several authentication failures in a short window of time.
- Ensure that all software has the latest security patches installed.
- Ensure that all anti-virus mechanisms are current and actively running.
- Monitor network and system logs to maintain a secure server.
- Backup server data.
- Maintain a test server and test functions prior to implementation.
- Use vulnerability scanners or other techniques to assess system vulnerabilities.

These recommendations come from the NIST Guide to General Server Security. Additional security controls may be necessary for a server depending on its function.

11 Mobile Devices

Mobile devices are easily lost or stolen due to their mobility and compact size. Therefore, additional precautions must be taken to protect institutional information that may be accessed from these devices.

Sensitive data should not be downloaded to mobile computing or storage devices. If it is necessary for sensitive data to be downloaded to a mobile device, the data should be encrypted. More information about what constitutes sensitive data and how it is to be handled can be found in Section 5 of the Information Security Users Guide titled, *Information Safeguards*.

All policies that pertain to email usages also apply when using institutional e-mail on a personal mobile device, as well. Email policies can be found on the ITSS Messaging Email Usage Policy webpage.

If using a mobile device for business purposes:

- Use a password, passcode or other form of authentication for the device.
- Do not use any device that has been rooted or jail broken.
- Adhere to all security policies.
- Sensitive data must be encrypted whether on a smartphone, laptop or removable media storage.
- Wipe all data from the device before it is retired, reused or donated.
- Use antivirus if it is available.
- Use location services selectively.

The Federal Communications Commission has created a smart phone security tool with steps to secure mobile phones, customized by mobile operating systems.

12 Firewall and Security Exceptions

In order to protect the confidentiality, integrity, and availability of information and information resources, the UNT System implements the principle of least privilege. Firewalls managed by ITSS will be configured in a "default deny" configuration for ingress traffic. Exception requests must support the mission of UNT System institutions. Exceptions must be approved by the UNTS Chief Information Security Officer (CISO) and the appropriate institutional CIO. The exception process is found in the ITSS Firewall Exception Process document.

13 System Security Review Procedures

Before a new system or application is adopted, acquired or integrated in to the ITSS computing infrastructure, ITSS Information Security must perform a security assessment. To request a security assessment, complete the ITSS System Acquisition Survey and return it to your IT manager or ITSS Information Security staff.

14 Compliance with Laws and Standards

14.1 FERPA

14.1.1 Overview of the Law

The Family Educational Rights and Privacy Act (FERPA) is a law that allows parents the rights of access to their child's education records, to have records corrected if necessary, and to have some control over what personally identifiable information is disclosed from those records. The rights transfer to the student once the student reaches the age of 18, or attends a postsecondary institution. Parents may have access to the information, if the student is claimed as a dependent by either parent for federal tax purposes.

Permission must be granted by the student before school records can be shared. Disclosure without consent of the student is allowed in specific circumstances, such as to school employees who have a legitimate educational interest, other schools where the student intends to enroll, accrediting organizations, certain government officials, for legal matters, among others.

Directory information is information that is considered harmless if disclosed and can be disclosed without consent. Directory information includes the student's name, address, university assigned e-mail, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of athletic team members, dates of attendance, enrollment status, degrees and awards received, expected graduation date, dissertation and thesis titles, most recent previous school attended and photograph.

Students can request that their directory information be withheld from public disclosure. The lists of students who have made such a request are identified within the Enterprise Information System (EIS).

More information about the law can be found in the links in the "Reference" section below.

If a student believes that their rights have been violated under FERPA regulations, they can file a complaint with the U.S. Department of Education. The Department of Education will investigate timely complaints with reasonable cause and inform the school of any steps it must take to come into compliance with the law.

14.1.2 Obligations of UNT System Institutions

Under the UNT System Information Security Standards and Practices Guide, educational records are classified as Category I information requiring a high level of security controls. Custodians and owners of educational records must follow these security controls concerning backups, change management, malware protection, physical security, system hardening, security monitoring and audit as a part of their overall information security plan.

Additional obligations are that students must be informed about their rights under FERPA.

All employees of a UNT System institution who regularly deal with student information should attend FERPA training, which is available through the Registrar's Office. Please contact the Registrar's Office for additional information or see the following websites:

- UNT Dallas Registrar's Office FERPA Information
- UNT Denton Registrar's Office FERPA Information
- UNT HSC Registrar's Office FERPA Information

14.2 HIPAA

14.2.1 Overview of the Law

The federal Health Insurance Portability and Accountability Act (HIPAA) and the Texas Medical Records Privacy Act, as well as the Family Educational Rights and Privacy Act (FERPA), govern how UNT System institutions protect health information. This document gives an overview of HIPAA and the Texas Medical Records Privacy Act along with the procedures required to protect individual's health information.

HIPAA provides a basic level of privacy of an individual's health care information. Protected Health Information (PHI) includes individually identifiable health information that a UNT System institution may receive electronically, on paper or verbally. It applies to health care providers, health plans, and processors of health insurance claims. In 2009, the Federal Government expanded these protections with the Health Information Technology for Economic and Clinical Health Act (HITECH) to apply to business associates and increased the notification requirements and penalties for violations.

HIPAA Privacy Standards pertain to the protection of an individual's health information and apply to electronic, paper or verbal information. HIPAA Security Standards are rules for covered entities to protect electronic-PHI and fall into three categories: administrative safeguards, physical safeguards, and technical safeguards.

In 2011, the state of Texas added further protections with the Texas Medical Records Privacy Act. This act broadens privacy responsibilities beyond health care providers,

health plan providers and insurance processors to business, individuals and organizations that collect, evaluate, use, store or transmit PHI. The Texas Medical Records Privacy Act requires verified training for employees of covered entities no later than the 60th day of employment and to be completed again at least once every 2 years. Because it is more stringent than the federal HIPAA law, the requirements of the state law prevail.

The HIPAA privacy rule excludes educational records that are protected under FERPA. Therefore healthcare records of a student who receives medical care from a health clinic run by a postsecondary institution are considered educational or treatment records under FERPA, and are not subject to HIPAA or the Texas Medical Records Privacy Act.

Violations of HIPAA can range from $100 per violation to $1.5 million depending on the nature and extent of the breach, harm done by exposure and other factors. Penalties cannot be imposed if the violation is corrected within 30 days and was not due to willful negligence.

The penalties for violations of the Texas Medical Records Privacy Act range from $5000 each violation per year if they are due to negligence; $25,000 if they were knowingly committed; and up to $250,000 if done for financial gain.

14.2.2 Obligations of UNT System Institutions

Anyone handling PHI protected under HIPAA must adhere to the following rules:

- Share PHI only on a need-to-know basis with authorized individuals.
- Get written authorization for use or disclosure of PHI for anything other than direct care or treatment.
- Use and disclose only what is minimally necessary.
- Use only authorized systems for processing, storing or entering PHI.
- Securely transmit all PHI by following the “UNT System Information Security Standards and Practices Guide.”
- Dispose of PHI securely by shredding, or rendering it unreadable.
- Report lost or stolen PHI immediately to your helpdesk or ITSS Information Security.

Under the UNT System Information Security Standards and Practices Guide, medical records, whether protected under FERPA or HIPAA, are classified as Category I information requiring a high level of security controls. Custodians and owners of medical records must follow these security controls concerning backups, change management, malware protection, physical security, system hardening, security monitoring and audit as a part of their overall information security plan.

14.3 Payment Card Industry Data Security Standards (PCI-DSS)

Any department or organization of UNT System institutions that accept payment cards or handle cardholder data must be in compliance with the payment card policy of its institution and the Payment Card Industry Data Security Standards (PCI DSS).

The PCI DSS applies to any merchant that accepts or processes payment cards. The PCI DSS covers twelve requirements, each with multiple components that align with best practices of security. The twelve requirements are:

1. Establish and maintain a firewall
2. Do not use vendor-supplied defaults for security
3. Protect stored cardholder data
4. Encrypt cardholder data that is transmitted across public networks
5. Use and regularly update anti-virus software or programs
6. Establish and maintain secure systems and applications
7. Restrict access to cardholder data to a need-to-know basis
8. Provide a unique ID for everyone requiring access
9. Restrict physical access to cardholder data
10. Track and monitor all access to cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for all personnel.

A part of PCI DSS requirements is to complete an annual Self-Assessment Questionnaire (SAQ) and attestation of compliance. Merchants found to be out of compliance may lose the right to accept credit cards until compliance has been established. Additionally, in the event of a breach, organizations out of compliance could be levied significant fines by the individual payment card brands.

All merchants should work with the appropriate financial office of their institution, their departmental IT manager and ITSS Information Security to resolve any compliance concerns.

15 Account Provisioning and Access

Access to IT resources should be provided using the principle of least privilege and removed or altered as an employee or other person-of-interest's roles or status changes. ITSS has created a Guide for Departments to determine the appropriate

actions to be taken and the responsible parties for these actions for granting access to various ITSS Services.

Regular security administrative and security reviews of access privileges should be conducted by information custodians, information owners, IT managers, and resource owners to ensure that only appropriate users have current access.

16 Encryption

UNT System information safeguards require that all laptops be encrypted with the full disk encryption product managed by ITSS Information Security. This is necessary so that the resources and processes exist for password reset, data recovery and forensic operations.

The IT managers are responsible for determining which machines should be encrypted based on content, UNT System or compliance polices.

Mobile devices accessing UNT System resources that support data-at-rest encryption must have encryption enabled. Any non-encrypted portable device should not contain any sensitive or protected information. As a best practice, sensitive or protected information should only be stored on secured systems.

ITSS Information Security hosts and manages the central key management server used to provide encryption services to all Windows and Mac OS X operating systems. Deployment and management of encryption is done through the centrally managed server. Training is available for IT managers as requested.

17 Log Management

Local logging of session data is required for systems that provide services to users. These machines must also sync with a time source (Network Time Protocol (NTP), time.nist.gov) on a regular basis. It is the responsibility of the service owner to ensure that logs exists that reflect security controls, user information, Internet Protocol (IP) source and destination information, date and time stamps, and logon and logoff times. Logging should be enabled on systems that contain information that would be required to perform root cause analysis of a security incident. Logs should be kept for a reasonable amount of time and for a minimum of 30 days, although 90 days is recommended. If the service is regulated by a compliance standard then that standard

is to be used. Logs should be routinely reviewed by the system administrator to detect abnormalities.

If a service provider is involved in a security incident and the administrator is unable to determine further information related to the incident, then the administrator becomes responsible.

ITSS Information Security may ask that critical systems forward their logs to a centralized log repository.

18 Web Application Security

The purpose of implementing web application security procedures is to ensure that websites, web applications and web services are secured appropriately. These procedures apply to all entities that publish or administer institutional information on all new and current websites, web applications and web services at UNT System institutions.

UNT System institutions must consider the Open Web Application Security Project's (OWASP) Top 10 Application Security Risks (2013) and establish guidelines for protecting web applications. The OWASP risks are identified below and can be viewed in more detail on OWASP's main website.

1. Injection
2. Broken Authentication and Session Management
3. Cross-Site Scripting (XSS)
4. Insecure Direct Object References
5. Security Misconfiguration
6. Sensitive Data Exposure
7. Missing Function Level Access Control
8. Cross-Site Request Forgery (CSRF)
9. Using Components with known vulnerabilities
10. Invalidated Redirects and Forwards

Note that these are only the top 10 security issues and serve as a basic guideline. There are hundreds of potential security flaws that need to be considered in order to adequately minimize security vulnerabilities.

19 Patch Management

Vendor supplied software should be maintained at a level supported by the vendor. Security patches should be applied in a timely manner following vendor recommended schedules, if available. Special attention is needed to keep all operating systems and applications up to date. Programs commonly found to be outdated include Java, Adobe, Firefox, Flash, and Shockwave. If a system can be configured to automatically update patches, then it should be configured as such.

Where possible, patching should be centrally managed with the ability to provide auditable update logs and alerts for out of date systems. System administrators should confirm the deployment and successful installation of patches, and should follow change management procedures. Unpatched machines that pose a high risk to the enterprise are subject to be removed from the network.

Special consideration should be made for operating system software. As system vulnerabilities become known and patches become available, the risk of installing the patch should be weighed against the risks of the vulnerabilities. Patches should be tested prior to installation to avoid any unwanted consequences. If no patch is available for a known vulnerability, other compensating controls should be considered.

20 Disaster Recovery and Business Continuity Planning

Business continuity and disaster recovery planning is required for institutions of higher education. Plans should include a business impact analysis, risk assessment, implementation maintenance, testing of the plan, and a disaster recovery plan.

All departments are responsible for maintaining documentation of services provided by the department that enable a recovery of its business functions and technology. The plan should act as a guideline for processing and coordinating activities. Checklists, flowcharts and diagrams should be included from the recovery team for supporting documentation. Templates are available at:

https://myunt.sharepoint.com/:w:/r/sites/DRBCP/ITSS%20DR%20Documentation/Templates/DRP- Checklist-SOP-Template.docx?d=wadebea2c4a1e466d93a9a75bfdece5f3&csf=1&e=d89HRz

https://myunt.sharepoint.com/:w:/r/sites/DRBCP/ITSS%20DR%20Documentation/Templates/DRP- Flowchart-SOP-Template.docx?d=waad041bd433242dd9d1d83d8c950bd6c&csf=1&e=64UPqN

https://myunt.sharepoint.com/:u:/r/sites/DRBCP/ITSS%20DR%20Documentation/Templates/DRP%20Flowchart%20Example.vsd?d=w17b34f9298e0402fa5ec774eeaa5e885&csf=1&e=BTCiKk

21 Incident Response

ITSS Information Security provides incident response services to UNT System institutions. This service is governed by the Information Security Handbook, and the Texas Administrative Code (202).

Procedures

1. Contact Information Security

To contact the ITSS Information Security team, please email security@untsystem.edu, put in a ticket, or call (940) 369-7800. We typically respond as soon as we are notified.

2. Identification

Once an incident has been identified, the person identifying the problem should:

- Contact information security to begin incident handling.
- Determine the validity of the incident.
- Define the scope of the incident.

In addition, the ITSS Information Security team will:

- Assemble a CERT team.
- Coordinate the communication amongst the CERT team.
- Manage the incident handling process.

3. Containment

Once the incident has been validated, containment should begin immediately. The containment process may include the following steps coordinated between the assets owner and ITSS Information Security:

- Collect any live data that might be relevant to the case.
- Inform stakeholders that the system or application will be offline.
- Remove the compromised system or application from public consumption.
- Collect relevant system forensic data.
- Mitigate the problem.
- Backup any valuable data or resources associated with the compromised system.

4. Investigation

For assets that are mission critical, have a high impact, or contain legally protected data, the investigative phase of the incident handling process will include a detailed analysis

of the case to determine the extent of the compromise, the nature of the problem, the steps needed to remediate the problem and prevent it from happening in the future, and the necessity to disclose the incident to the stakeholders.

The investigation phase includes the following tasks, managed by the CERT leader:

- Forensic analysis of the data collected from the compromised system.
- Construction of an incident report.
- Drafting of remediation recommendations.
- Reporting the incident to management.

ITSS Information Security will provide forensic examination, to the best of their ability. When the scope of the examination expands beyond the skillset of the ITSS Information Security team, the representative for the involved technology will be called upon for assistance.

There is no set timeframe on the investigation as it depends on the impact and scope of the compromise.

5. Recovery

The recovery phase of the incident is concerned with restoring the system or application to a working state and taking necessary actions, such as disclosure of the incident that resulted from the compromise. The following tasks occur during the recovery phase and are the responsibility of the assets owner:

- Repairing or rebuilding the system or application that was compromised.
- Restoring system data to a known good state.
- Validating that the problem that caused the incident has been addressed.
- Communicating to users that the system is back online.
- Taking any appropriate administrative actions related to the incident.

ITSS Information Security will disclose the incident to affected users if necessary.

6. Follow-Up

The follow up phase of the incident handling process can involve all involved parties and will address any remaining administrative activity related to the incident and allow us to reflect on how the experience may help us prevent similar incidents from happening in the future and adjust our procedures to make the process better. Tasks in this phase may include:

- Conducting a “lessons learned” meeting with the people involved in the incident.
- Reporting the incident to DIR.

- Adjusting our policies, procedures, standards, and tools to improve the security of our systems.

22 Incident Communications Plan

All institutions should develop an Incident Communications Plan to be used in the event of a major incident. The plan is necessary to ensure timely and accurate communications about an incident to all customers and to improve communications with stakeholders.

23 Anti-virus and malware

ITSS Information Security hosts and manages the central management servers necessary to provide anti-malware protection to enterprise assets. All capable systems must run the central management agent (Currently the McAfee Agent). This is required for security, management, and compliance reporting.

All capable systems must run current anti-virus software provided by ITSS Information Security (Currently McAfee Virus Scan) with a minimum policy set as stated in the "Minimum Operating System Standards" document.

24 Email Security

Email systems are provided by the UNT System to support the mission of the system and its institutions. There is no expectation of privacy when using a UNT System institution email system. Therefore, sensitive data should never be sent via email. This includes, but is not limited to, social security numbers, payment cardholder data, and protected health information. General policies about email can be found in the UNT System Email Usage Policy.

Phishing is an attempt to obtain sensitive information through a deceptive email. Some of the attempts can be quite convincing with logos or disclaimers taken from legitimate websites. There are several things you can look for to determine if a request is a phishing scam. If you have doubts about an email sent to you or believe that you may have given out sensitive information contact your computer support personnel, or email security@untsystem.edu.

If you respond to a phishing attempt or suspect that your email has been hacked, follow the steps given on the ITSS Messaging webpage.

25 Network Security

Only devices that have been approved by ITSS may be connected to the network.

Services that require public access should be deployed in the network “de-militarized zone” or DMZ. The DMZ is a perimeter network that allows open access to our public sites and adds an additional layer to of security to protect our sensitive data. Any system in the DMZ should not contain any sensitive or protected information.

26 Vulnerability Assessments

The ITSS Information Security team provides on-demand comprehensive vulnerability scanning services for IT managers. Several tools are used depending on the type of scan requested. Examples include but are not limited to non-credentialed and credentialed operating system scans, port scans, and web application scans. Once completed, an analyst will review the results and work with the IT manager to provide guidance and assist with addressing any issues found as long as it is within the expertise of the security team. The results are provided as-is.

Systems on datacenter networks are subject to be scanned by ITSS Information Security on a weekly basis.

Authenticated vulnerability scans are to use an account that is not used for any other purpose and should be an Active Directory account that has the password changed often.

27 Change Management

Formal change management procedures that are documented and enforced protect the integrity of information resources. ITSS manages the changes in the IT environment through its change management process that are established by the Service Management team.

28 Sanctions

Sanctions for the violation of UNT institutional policies and applicable state or federal laws are cited in the in the various institutions Policies defining employee and student codes of conduct and employee information. Penalties for violations range from the loss of computing resources privileges to the dismissal from the university, and may also include civil action or prosecution. Institutional policies can be found at these institution webpages:

UNT
HSC
UNT Dallas

29 References

29.1 UNT Computing Policies, Guidelines, and Handbooks

29.1.1 Computing Policies

- UNT System Information Security Regulation: https://www.untsystem.edu/sites/default/files/01_About/06.1000_information_security_00084028.pdf
- UNT Policy 14.001 Student E-Mail: http://policy.unt.edu/policy/14-001
- UNT Policy 14.002 Information Security Policy: http://policy.unt.edu/policy/14-002
- UNT Policy 14.003 Computer Use Policy: http://policy.unt.edu/policy/14-003
- UNT Policy 14.004 Network Connections Policy: http://policy.unt.edu/policy/14-004
- UNT Policy 14.005 Electronic and Information Resources Accessibility: http://policy.unt.edu/policy/14-005
- UNT Policy 14.006 Use of University Non-Wireless and Wireless Telephones, Telephone Lines, Fax Machines and Personal Computing Devices: http://policy.unt.edu/policy/14-006
- UNT Policy 14.007 Web Publishing: http://policy.unt.edu/policy/14-007
- UNT Policy 14.008 Web Accessibility: http://policy.unt.edu/policy/14-008
- HSC Acceptable Electronic Communications Use Policy 04.301: https://unthsc.policytech.com/dotNet/documents/?docid=479
- HSC Server Management and Security Policy 04.302: https://www.unthsc.edu/administrative/wp-content/uploads/sites/23/Server_Management_and_Security_Policy.pdf 0Security%20Policy.pdf

- HSC Data Integrity and Classification Policy 04.304: https://unthsc.policytech.com/dotNet/documents/?docid=168
- HSC Web Policy 04.305: https://unthsc.policytech.com/dotNet/documents/?docid=176
- HSC Transmission of Health Information via PDA Policy 04.308: https://unthsc.policytech.com/dotNet/documents/?docid=175
- HSC Information Security Policy: https://unthsc.policytech.com/dotNet/documents/?docid=480
- UNTD Electronic Communication Policy 14.001: http://www.untdallas.edu/sites/default/files/page_level2/pdf/policy/14.001%20Electronic%20Communication.pdf
- UNTD Internet Use Policy 14.002: http://www.untdallas.edu/sites/default/files/page_level2/pdf/policy/14.002%20%20Internet%20Use.pdf
- UNTD Portable Computing Policy 14.003: http://www.untdallas.edu/sites/default/files/page_level2/pdf/policy/14.003%20Portable%20Computing.pdf
- UNTD Use of Licensed Commercial Software Policy 14.004: http://www.untdallas.edu/sites/default/files/page_level2/pdf/policy/14.004%20Use%20of%20Licensed%20Commercial%20Software.pdf
- UNTD Network Access Policy 14.005: http://www.untdallas.edu/sites/default/files/page_level2/pdf/policy/14.005%20Network%20Access.pdf
- UNTD Password Protection Policy 14.006: http://www.untdallas.edu/sites/default/files/page_level2/pdf/policy/14.006%20Password%20Protection.pdf
- UNTD Privacy Policy 14.007: http://www.untdallas.edu/sites/default/files/page_level2/pdf/policy/14.007%20Privacy.pdf
- UNTD Acceptable Use Policy 14.008: http://www.untdallas.edu/sites/default/files/page_level2/pdf/policy/14.008%20Acceptable%20Use.pdf
- UNTD Physical Access Policy 14.009: http://www.untdallas.edu/sites/default/files/page_level2/pdf/policy/14.009%20Physical_Access.pdf
- UNTD Use of University Non-Wireless Telephones, Telephone Lines, Fax Machines and Computers Policy 14.011: https://www.untdallas.edu/sites/default/files/page_level2/hds0041/pdf/14_011_use_of_non-wireless_telephones_00168904xc146b.pdf
- UNTD Information Security Policy 14.012: https://www.untdallas.edu/sites/default/files/page_level2/hds0041/pdf/14.012_information_security.pdf

29.1.2 Computing Guidelines

- Remote Access Guide
  https://itss.untsystem.edu/sites/default/files/campus_vpn.pdf
- Web Hosting Policy:
  https://itss.untsystem.edu/divisions/ets/cws/web-hosting-policy
- ITSS Messaging Email Usage Policy
  http://itss.untsystem.edu/services/messaging-services/unt-system-email-usage-policy.

29.1.3 Handbooks and University Policy Offices

- UNT System Information Security Handbook
  https://itss.untsystem.edu/divisions/mrs/is/articles-and-resources/unt-system-information-security-handbook handbook.pdf
- UNT University Policy Office
  http://policy.unt.edu
- HSC Policies
  https://www.unthsc.edu/administrative/institutional-compliance-office/unt-health-science-center-policies/
- UNT Dallas University Policies
  https://www.untdallas.edu/hr/upol
- UNT Code of Student Conduct:
  https://policy.unt.edu/policy/07-012_North%20Texas%20Code%20of%20Student%20Conduct.pdf
- UNT Health Science Center Student Code of Conduct and Discipline:
  https://unthsc.policytech.com/dotNet/documents/?docid=265
- UNT Dallas Code of Student's Rights, Responsibilities and Conduct:
  https://www.untdallas.edu/sites/default/files/page_level2/pdf/policy/7.001_code_of_students_rights_responsibilities_and_conduct.pdf
- UNT System Information Security Standards and Practices Guide:
  https://itss.untsystem.edu/sites/default/files/Information%20Security%20Standards%20and%20Practices.pdf

29.2 State and Federal Laws

- Information Security Standards -Texas Administrative Code Title 1, Part 10, Chapter 202:
  https://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=%2010&ch=202
- Computer Crimes- Texas Penal Code, Chapter 33:
  http://www.statutes.legis.state.tx.us/docs/PE/htm/PE.33.htm

- Computer Fraud and Abuse Act of 1986- U.S. Penal Code, Title 18, Section 1030: http://uscode.house.gov/view.xhtml?req=(title:18%20section:1030%20edition:prelim)
- Family Educational Rights and Privacy Act: http://www.unt.edu/ferpa/ http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html http://policy.unt.edu/policydesc/ferpa-policy-18-1-9
- UNT Dallas Registrar's Office FERPA Information: https://registrar.untdallas.edu/ferpa
- UNT Denton Registrar's Office FERPA Information: http://www.unt.edu/ferpa/
- UNT HSC Registrar's Office FERPA Information: https://www.unthsc.edu/students/registrar/ferpa/
- Fraud and related activity in connection with computers- U. S. Penal Code, Title 18, Chapter 47: http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter47&edition=prelim
- Fraud and False Statements, Section 1030: http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter47&edition=prelim
- 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/Public Information Act: https://www.texasattorneygeneral.gov/open-government/office-attorney-general-and-public-information-act http://dentoncounty.com/Pages/Open-Records-Act.aspx
- 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): https://www.dol.gov/agencies/ebsa/laws-and-regulations/laws/hipaa
- GLBA (Gramm-Leach-Bliley Act): http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act

29.3 UNT System Computing Resources and Support

- UNT System IT Shared Services (ITSS): http://itss.untsystem.edu
- UNT System Information Security: http://security.untsystem.edu

- Antivirus Downloads:
  http://itss.untsystem.edu/antivirus-download
- UNT University Information Technology:
  http://it.unt.edu
- UNT UIT Helpdesk:
  http://www.unt.edu/helpdesk
- UNT HSC Helpdesk:
  http://helpdesk.hsc.unt.edu
- UNT Dallas Helpdesk:
  https://www.untdallas.edu/itss/services/helpdesk
- UNT Distributed IT Support Groups:
  http://www.unt.edu/helpdesk/netman/
- UNT Police Department:
  http://www.unt.edu/police
- UNT Dallas Police Department:
  http://dallas.unt.edu/police
- UNT HSC Police Department:
  http://hsc.unt.edu/police
- Standards for Granting and Removing Access to Information Resources: Guide for Departments:
  https://itss.untsystem.edu/sites/default/files/Standards%20for%20Granting%20and%20Removing%20IT%20Access.pdf
- ITSS Firewall Exception Process:
  https://itss.untsystem.edu/sites/default/files/Firewall%20Exception%20Process.pdf

29.4 Other Helpful Sites

- OWASP – Open Web Application Security Project
  https://www.owasp.org
- NIST Guide to General Server Security:
  http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf
- Federal Communications Commission Smart Phone Security tool:
  http://www.fcc.gov/smartphone-security

30 Contact Information

More information can be found at http://security.untsystem.edu.
Send direct questions, comments or incident reports to: security@untsystem.edu or (940) 369-7800.