Policy Number and Chapter:	**14.003**	Information Technology
Policy Title:	**Acceptable Use**	

Policy Statement. The University of North Texas (UNT) provides Information Resources for employees, students and authorized individuals to use in conducting official University business and for other purposes as authorized in this policy.

Application of Policy. This policy applies to all users granted access to University Information Resources, including but not limited to students, faculty, staff, and guests.

Definitions.

1. Access. "Access" means the physical or logical capability to view, interact with, or otherwise make use of information resources.

2. Child Email Domain. "Child Email Domain" means the part of an email address that is used to create a secondary name associated with the organization to which the email is assigned or owned, e.g., "meangreensports" is the child domain in "@meangreensports.unt.edu".

3. Cloud Service. "Cloud Service" means a service made available to a user by a third-party provider via the Internet in an externally managed data center or computing facility.

4. Confidential Information. "Confidential Information" means information that must be protected from unauthorized disclosure or public release, based on state or federal law or other legal agreement (e.g., the Texas Public Information Act, and other constitutional, statutory, judicial, and legal agreement requirements).

5. Data. "Data" means all information, regardless of size or storage media, including email messages, system logs, and software (commercial or locally developed).

6. Email Domain. "Email Domain" means the name used in an email address that identifies the organization to which the email is assigned or owned.

7. Employee. "Employee" means an individual who is employed full-time, part-time or in a temporary capacity as faculty, staff, or who is required to be a student as a condition of employment.

8. Information Resources. "Information Resources" means the procedures, equipment, and software employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information.

9. Information Owner. "Information Owner" means a person with operational authority for information who is responsible for authorizing controls for generation, collection, processing, access, dissemination, and disposal of that information.

10. Least Privilege. "Least Privilege" means the security principle that requires the application of the most restrictive privileges needed for performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

11. Personally Identifiable Information. "Personally Identifiable Information" means information that alone or in conjunction with other information identifies an individual, including an individual's name, social security number, date of birth, or government-issued identification number; mother's maiden name; unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; unique electronic identification number, address, or routing code; and telecommunications access devices as defined by Section 32.51 of the Texas Penal Code.

12. Primary Email Domain. "Primary Email Domain" means the name used at the end of an email address that identifies the name of the organization to which the email is assigned or owned, e.g., "@unt.edu".

13. Users. "Users" means individuals or automated applications that are authorized to access information or information resources in accordance with the information owner-defined controls and access rules.

Procedures and Responsibilities.

A. Guidelines

The following guidelines set out the permissible use of University Information Resources:

1. **Authorized Use:** Individuals may use University Information Resources for the purpose of conducting University business or as otherwise set out in this policy.

   a. The University may limit the use of Information Resources to specific research, teaching missions or other purposes at its sole discretion, and may otherwise restrict or revoke authorization at any time.

   b. University students may use University information resources for school-related and personal purposes in accordance with this policy and other applicable University policies, and state and federal law, provided personal use does not result in any additional costs to the University.

   c. University employees and authorized individuals may use Information Resources in accordance with this policy and other applicable University

policies, and state and federal law. Incidental personal use of Information Resources by employees and authorized individuals is permitted, subject to review and reasonable restrictions by the employee's supervisor, provided the use does not interfere with the performance of job responsibilities and does not result in any additional costs to the University.

d. The University may provide Information Resources access to retirees, visiting scholars, vendors and other external users as necessary to advance the mission and operation of the University. Information Resources must be used in accordance with this policy, any contractual obligations, the UNT System Information Security Handbook, and other University policies and state and federal law.

2. **Freedom of Expression:** University information resources are a non-public forum unless otherwise expressly designated by the appropriate University official. The University will not restrict access to information through its Information Resources based on content or viewpoint as long as the information meets legal standards. However, the University reserves the right to limit, restrict, or deny Information Resource privileges or access for those who violate state and federal laws and other University policies.

3. **Privacy.** Users of University Information Resources have no expectation of privacy regarding information collected, recorded, processed, stored, displayed, retrieved or transmitted using University Information Resources beyond that which is expressly provided by applicable privcy laws. The University may monitor, access, and review any such information for University purpose or duties. This information also may be subject to review or disclosure in accordance with the following:

   - Texas Public Information Act and other laws;
   - Administrative review for security or compliance purposes;
   - Computer system maintenance;
   - Law enforcement and other investigations;
   - Audits, and
   - As otherwise required to protect the reasonable interests of the University and other users of Information Resources.

   The University does not guarantee the protection of electronic files, data or other information, including e-mails, from unauthorized third-party access.

4. **Intellectual Property.** Works created or communicated through University Information Resources are subject to University copyright policy and applicable copyright laws. University Information Resources may not be used to violate

intellectual property rights, including downloading or distributing copyrighted material without proper authorization from the copyright holder.

5. **Valuable Assets**. Information Resources purchased or leased by the University are the property of the University or the vendor from whom the resource is leased. Any unauthorized access, use, alteration, duplication, destruction, or disclosure of these assets may be a criminal offense under state and federal laws.

6. **Transportation**. University Information Resources and data contained in the Information Resources may not be transported domestically or internationally without appropriate authorization, including authorization required under export control laws as applicable.

7. **Export Controls**. Certain University information may not be accessed by or transmitted to foreign persons within or outside the United States or to U.S. citizens in foreign countries. Please see UNT Policy 13.010, Export Controls, for more information.

B. Information and Technology Use

1. **Security.**
   a. The use of Information Resources and data must comply with the UNT Information Security Policy, the UNT System Information Security Handbook, and applicable information security standards and privacy policies. Access, usage, and treatment of Information Resources and data must not violate the confidentiality, integrity, or availability of these assets, and must adhere to the principle of least privilege to ensure that access is assigned as appropriate for tasks that are to be performed and removed when no longer necessary.

   b. Retirees, visiting scholars, vendors and other external users may obtain access to Information Resources based on their role.

   c. Access and use of data must be approved by the information owner prior to use, processing, and installation.

   d. University Information Resources and data must be encrypted if transported domestically or internationally.

   e. Individuals that use or access confidential or personally identifiable information must complete security and data privacy training as appropriate for the type of data or information that is approved prior to access.

   f. Upon termination, retirement, change in employment status, or cessation of an agreement or contract with the University, access to Information Resources and data must be terminated or modified in accordance with the new status

of the individual. University-owned accounts, data, email and Information Resources that were assigned to or used by a former employee, visiting scholar, vendor or other external user must be recovered and transferred to the former employing or hosting department for business continuity purposes.

2. **Email Use**.
   a. Email is the mechanism by which the University officially communicates with employees and students. Only email systems authorized by IT Shared Services may be used to send email communications on behalf of a University email domain. Third-party senders may not create an appearance that email sent by the third party is official University correspondence. Child email domains may be used by third-party mail senders if they are authorized by IT Shared Services. Automatic forwarding of bulk email to a third-party email system or third-party email address is prohibited.

   b. Email should not be used to store or transmit personally identifiable or confidential information to external parties unless the email is encrypted or secured in accordance with applicable University policies, laws and standards.

   c. Content contained within an employee's mailbox remains under the custody of the employing department and will be retained by the department when an employee separates from the department, or when a change in employment status occurs. It is the responsibility of a department to archive email contained in the mailbox of a former employee or a retired employee for business continuity purposes.

   d. An employee may request a new non-employee email account upon retirement. Emeritus faculty may retain their University email account upon retirement.

3. **Cloud Services**. The use of cloud services must be compliant with University policies and applicable laws governing security, privacy, procurement, administration, supplier service relationships, export controls, and appropriate use of Information Resources and data. University data may not be transmitted, processed or stored by a third party until Information Security and the appropriate IT groups have conducted a security assessment. Cloud service providers must ensure the confidentiality, integrity and availability of data, information, and services that they provide.

4. **Websites**. Website usage and web administration must comply with University policies, standards, and applicable laws, including those that address web accessibility, security, and privacy.

5. **Personally Owned Accounts, Software and Contracted Services**. Personally owned accounts, software, and contracted services may not be used to conduct

university business, including transmission, storage, or processing of data that is owned by the University.

6. **Network Access**. IT Shared Services is responsible for ensuring that networks are administered in a manner that facilitates availability to all users. Only authorized devices may connect to University networks. The introduction of devices or information resources that negatively affect the behavior or security of the network, or violate University policies, is prohibited.

7. **Remote Access**. Users that remotely access University information resources from an external location must ensure that information resources used at the remote location comply with the UNT System Information Security Handbook, including the requirements that address secure network and access control mechanisms, secure exchange of information transferred between the remote location and the University through use of the University VPN, current maintenance of information resources, and prevention of unauthorized viewing of confidential and personally identifiable information. Users must also comply with all export control requirements for any information accessed while outside the United States.

C. **Responsibilities.**

1. Users shall use University Information Resources responsibly, respecting the needs of other Users.

2. Users are responsible for any usage of his or her account, Information Resources or data entrusted to him or her.

3. Users must maintain the secrecy of their passwords. If a user suspects their password is compromised, they must reset it as soon as possible.

4. Users must report any misuse of Information Resources or violations of this policy to their supervisor, department head, or to the Chief Information Officer.

5. Users are responsible for obtaining and adhering to relevant Information Resources policies.

6. Users must comply with applicable laws and regulations, contractual agreements, institutional regulations and policies, licensing agreements and defined procedures.

7. Employees and contractors must complete annual security awareness training.

8. Users are responsible for reporting security incidents, including any potentially compromised accounts, suspected system irregularities, and/or vulnerabilities, to the UNT System Chief Information Security Officer.

9. Users must use Information Resources only for the purpose in which access has been authorized and only in the manner and to the extent authorized. The ability to access Information Resources does not, by itself, imply authorization to do so.

10. Supervisors are responsible for promptly informing University officials and information technology personnel when employment status changes occur, and when written agreements or contracts with visiting scholars, vendors, or other external users terminate in order to ensure that access to Information Resources are disabled or modified as appropriate.

D. Misuse of Information Resources.

The following actions constitute misuse of the University's Information Resources and are strictly prohibited for all Users:

1. Use of University Information Resources in support of or for illegal activities. Any such use will be reported to the appropriate University official and law enforcement authorities, as applicable. Criminal and illegal use may involve, but is not limited to, unauthorized access, intentional corruption or misuse of Information Resources, theft, obscenity, and child pornography.

2. Failure to comply with laws, policies, procedures, license agreements, and contracts that pertain to and limit the use of the University's Information Resources.

3. Abuse of Information Resources, including, but not limited to:

    a. Any act which endangers or damages specific software, hardware, program, network or system as a whole, whether located on campus or elsewhere on the global Internet;
    b. Creating or purposefully allowing a computer malfunction or interruption of operation;
    c. Injecting a virus or other malware into an Information Resource;
    d. Sending a message with the intent to disrupt University operations or the operations of outside entities;
    e. Printouts that tie up Information Resources for an unreasonable time period to the detriment of other authorized users;
    f. Sending spam messages;
    g. Computing tasks that consume an unreasonable amount of resources, either on or off campus, to the detriment of other authorized users; and
    h. Failing to adhere to usage limitations that apply at particular computer facilities on campus.

4. Use of University Information Resources for personal financial gain unrelated to University responsibilities and job expectations or for a personal commercial

purpose.

5. Failure to protect the privacy of a password, account or confidential information from unauthorized use or access.

6. Permitting someone to use another's account or credentials, or using someone else's account or credentials.

7. Unauthorized use, access, reading, or misuse of any electronic file, program, network, or system.

8. Unauthorized use, access, duplication, disclosure, alteration, damage, misuse, or destruction of data contained in any electronic file, program, network, or University hardware or software system.

9. Unauthorized duplication and distribution of commercial software and other copyrighted digital materials. The unauthorized duplication and distribution of software and other materials protected by copyright (including copyrighted music, graphics etc.) is a violation of copyright law and this policy. Exceptions to this violation include specific authorization by the copyright holder or use protected by the fair use provisions of the copyright law.

10. Infringing upon the copyright, trademark, patent, or other intellectual property rights of others through the use of institutionally owned Information Resources.

11. Attempting to circumvent, assisting someone else, or requesting that someone else circumvent any security measure or administrative access control that pertains to University data or Information Resources.

12. Use of University Information Resources in a manner that violates other University policies.

13. Use of University Information Resources for the transmission of commercial or personal advertisements, solicitations, or promotions in accordance with University's ethics policy.

14. Use of University Information Resources for transmission of political material in accordance with University's ethics policy.

15. Installing unauthorized software or hardware that permits unauthorized access to institutionally owned information and Information Resources.

E. Access to University Information Resources

.The administrators of University Information Resources may provide University faculty, staff, students and other individuals access to University Information Resources in accordance with this policy when such access is appropriate to the individual's role or function at the University.

F. Disciplinary Actions

Failure to adhere to this policy may lead to the cancellation of the individual's account(s) and to other disciplinary action by the University. Additionally, individuals may be subject to possible civil and criminal action.

Responsible Party: Chief Information Officer

References and Cross-references.

Texas Administrative Code Title 1, Part 10, Chapter 202, Information Security Standards
Texas Administrative Code Title 1, Part 10, Chapter 206, State Websites
Business and Commerce Code Chapter 521, Identity Theft Enforcement and Protection Act
UNT System Information Security Handbook
UNT System Password Standards
UNT Policy 05.015, Ethics
UNT Policy 07.006, Free Speech and Public Assembly on Campus Grounds
UNT Policy 08.001, Copyright Compliance
UNT Policy 13.010 Export Control
UNT Policy 14.002, Information Security

Policy Contact:	Chief Information Security Officer
Approved Date	08/97
Effective Date	8/97; 8/01; 11/05
Last Revision:	8/01; 11/05; 02/17; 2/2021