Policies of the University of North Texas	Chapter 14
14.003 Computer Use	**Information Technology**

Policy Statement. The University of North Texas provides each of its authorized users with one or more computer accounts that permit use of the university's computer resources. Use of these resources is a privilege, not a right. When using these resources, individuals agree to abide by the applicable policies of the University, as well as federal, state and local laws. The University reserves the right at any time to limit, restrict or deny access to its computer resources, as well as to take disciplinary and/or legal action against anyone in violation of these policies and/or laws.

Application of Policy. Total University.

Definitions. None

Procedures and Responsibilities.

The policies and procedures which apply to users of University computer resources include, but are not limited to, this policy, as well as University policies against harassment, plagiarism, and unethical conduct and any procedures which govern computer usage at a particular facility on campus. Laws which apply to users of University computer resources include, but are not limited to, federal, state and local laws pertaining to theft, copyright infringement, insertion of viruses into computer systems, and other computer related crimes. This policy applies to all University computer resources, whether administered centrally or within a department, on-campus or remote, single or multi-user, mainframe or network server, etc. Computer resources include hardware, software, communications networks, electronic storage media, and manuals and other documentation. Data includes all files, regardless of size or storage media, including e-mail messages, system logs, and software (commercial or locally developed). For complete information concerning the use of Group E-mail, please refer to *Group E-Mail Guidelines*.

I. Principles. The following principles address the general philosophy of the University of North Texas on computer use and security. These principles apply to and are binding on all users of University computer resources:

A. Authorized Use: The University of North Texas provides computer resources for the purpose of accomplishing tasks related to the University's mission.

It should be noted that the use of some of the computers, networks, and software located on or off the University campus may be dedicated to specific research, teaching missions or purposes that limit their use or access.

Students, including registered students as well as incoming students who have paid their fees, shall be allowed to use the University's computer resources for school-related and personal purposes, subject to this policy and other applicable

University policies; state and federal law; and as long as personal use does not result in any additional costs to the University. Graduating students will have their computer accounts terminated after the next long semester. Non-enrolled continuing students may retain their computer account(s) for up to twelve months.

An employee of the University shall be allowed to use computer resources in accordance with this and other applicable University policies. Incidental personal use of computer resources by employees is permitted, subject to review and reasonable restrictions by the employee's supervisor; adherence to applicable University policies and state and federal law; and as long as such usage does not interfere with the employee's accomplishment of his or her job duties and does not result in any additional costs to the University. New employees shall gain immediate access to university computing resources upon the presentation of employment verification by the appropriate school, college, or department official. When an employee terminates employment for any reason other than retirement, his or her access to the University's computer resources will be terminated immediately unless specifically authorized by the Associate Vice President for Computing and Chief Technology Officer. Retired employees may retain access to computing services.

B. Freedom of Expression*:* Censorship is not compatible with the goals of the University of North Texas. The University will not limit access to any information due to its content as long as it meets the standard of legality. The University does reserve the right, however, to place reasonable time, place and manner restrictions on freedom of expression on its computer systems.

C. Privacy*:* Users of the University's computer systems should be aware that computer use may be subject to review or disclosure in accordance with the Texas Public Information Act and other laws; administrative review of computer use for security purposes or in regard to a policy or legal compliance concern; computer system maintenance; audits and as otherwise required to protect the reasonable interests of the University and other users of the computer system. Anyone using the University's computer systems expressly consents to monitoring on the part of the University for these purposes and is advised that if such monitoring reveals possible evidence of criminal activity, University administration may provide that evidence to law enforcement officials. Further, all users should understand that the University is unable to guarantee the protection of electronic files, data or e-mails from unauthorized or inappropriate access.

D. Intellectual Property: All members of the University community should be aware that intellectual property laws extend to the electronic environment. Users should assume that works communicated through the computer network are subject to copyright laws, unless specifically stated otherwise.

E. Valuable assets*:* Computer resources and data are considered valuable assets of the University. Further, computer software purchased or leased by the University

is the property of the University or the company from whom it is leased. Any unauthorized access, use, alteration, duplication, destruction, or disclosure of any of these assets may constitute a computer-related crime, punishable under Texas statutes and federal laws. University computer resources may not be transported without appropriate authorization.

II. Misuse of Computing Resources. The following actions constitute misuse of the University's computer resources and are strictly prohibited for all Users:

A. Criminal and illegal acts. University computer resources are not to be used in support of or for illegal activities. Any such use will be reported and dealt with by the appropriate University authorities and/or law enforcement agencies. Criminal and illegal use may involve, but is not limited to, unauthorized access, intentional corruption or misuse of computer resources, theft, obscenity, and child pornography.

B. Failure to comply with laws, policies, procedures, license agreements, and contracts that pertain to and limit the use of the University's computer resources.

C. Abuse of computer resources including, but not limited to, any act which endangers or damages specific computer software, hardware, program, network or the system as a whole, whether located on campus or elsewhere on the global Internet; creating or purposefully allowing a computer malfunction or interruption of operation; injection of a computer virus on to the computer system; sending a message with the intent to disrupt University operations or the operations of outside entities; print outs that tie up computer resources for an unreasonable time period to the detriment of other authorized users; computing tasks that consume an unreasonable amount of communications bandwidth either on or off campus to the detriment of other authorized users; and failure to adhere to time limitations which apply at particular computer facilities on campus.

D. Use of University computer resources for personal financial gain or a personal commercial purpose.

E. Failure to protect a password or account from unauthorized use.

F. Permitting someone to use another's computer account, or using someone else's computer account.

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

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

I. Unauthorized duplication and distribution of commercial software and other copyrighted digital materials. All commercial software and many other digital materials are covered by a copyright of some form. The unauthorized duplication and distribution of software and other copyrighted materials (including

copyrighted music, graphics etc) is a violation of copyright law and this policy. Exceptions to this are specific authorization by the copyright holder or use under the fair use provisions of the copyright law.

J. Attempting to circumvent, assisting someone else or requesting that someone else circumvent any security measure or administrative access control that pertains to University computer resources.

K. Use of the University computer system in a manner that violates other University policies such as racial, ethnic, religious, sexual or other forms of harassment.

L. Use of the University's computer system for the transmission of commercial or personal advertisements, solicitations, promotions, or employees' transmission of political material that is prohibited by the University's ethics policy (Policy 1.2.9) except as may be approved by the Office of the Associate Vice President for Computing and Chief Technology Officer.

III. Responsibilities of Users.

A. A user shall use the University computer resources responsibly, respecting the needs of other computer users.

B. A user is responsible for any usage of his or her computer account, computing resources or data entrusted to him or her. Users should maintain the secrecy of their password(s).

C. A user must report any misuse of computer resources or violations of this Policy to their department head or to the Office of the Associate Vice President for Computing and Chief Technology Officer.

D. A user must comply with all reasonable requests and instructions from the computer system operator/administrator.

E. When communicating with others via the University computer system, a user's communications should reflect high ethical standards, mutual respect and civility.

F. Users are responsible for obtaining and adhering to relevant network acceptable use policies including the Information Resources Security Policy and the Network Connections Policy.

IV. Responsibilities of Deans, Department Heads, and Supervisors.

A. Ensure that employees within a department receive opportunities to attend training courses that help them to comply with this policy and other applicable University policies.

B. Promptly inform appropriate computer system administrators when employees have been terminated so that the terminated employee's access to University computer resources may be disabled.

C. Promptly report ongoing or serious problems regarding computer use to the Office of the Associate Vice President for Computing and Chief Technology Officer.

V. Auditor Access of University Computing Resources. 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:

A. Internal Auditors from the University of North Texas:

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

2. Shall notify the Office of the Associate Vice President for Computing and Chief Technology Officer and the Office of the Vice Chancellor and General Counsel prior to accessing individual data files.

B. State and Federal Auditors. 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.

VI. Access to Services. The following chart delineates University of North Texas community members, their authorized computer resource access status, the duration of this status, and additional considerations.

Definitions: *Status Source* refers to the authoritative record for determination of university community membership. Authorized *General Access* users have UNT Helpdesk support, free Internet services (email, newsgroups, mailing lists, non-commercial personal web page space), General Access Lab admittance, CBT access, and license-restricted online Library resources. Authorized *Campus Network Access* users have connection privileges to university campus hardware and network backbone resources.

Multi-user host services are provided to University of North Texas faculty, staff, and students upon authorization of the system manager when such access is appropriate. Some remote services may be restricted by IP address.

	Status Source	*General Access*	*Campus Network Access*	*Service Duration*	*Notes*
Students (Undergraduate/Graduate)					
Registered UNT Students - Denton campus/Systems Center	student records	yes	yes	while continuing student	Some services (General Access Labs, CBT) require the presentation of a valid UNT ID and/or appropriate

					additional registration
UNT Health Science Center Students	HSC student records	no	no		
Registered UNT Students - Distributed Learning	student records	yes	yes	while continuing student	including web-based programs
Texas Academy of Math and Science [TAMS] Students	student records	yes	yes	while continuing student	
Universities' Center at Dallas - UNT registered	student records	yes	yes	while continuing student	
Universities' Center at Dallas - non-UNT registered	appropriate universities' student records	no	no		Exception: persons affiliated with contracted UNT services (for length of contract)
Collin County Community College Preston Campus - concurrent enrollment	CCCC and UNT student records	no	no		computing services being provided by CCCC as per agreement with UNT
People auditing UNT classes	associated department	no	no		
Conference and workshop participants (band camps, Summer Success etc.)	associated department	no	yes - as appropriate	length of event	
Faculty and Staff also registered as students	student records	yes	yes	while continuing student	When doing work as a *student* they do **not** get the extra privileges given to faculty/staff

UNT Alumni	student records	no	no	retain **internet account only** for one long semester after graduation	when no longer classified as a non-enrolled continuing student.
Non-enrolled continuing students	student records	internet account only	no	may retain internet account up to twelve months	
Continuing Education students	Continuing Education office	contracted	contracted		
UNT Applicants	student records	no	may obtain a student email account and access to the central web portal		
Faculty and Staff					
UNT fulltime/part-time faculty and staff - Denton campus/Systems Center	Payroll Office	yes	yes	immediately upon termination	New employees may receive access to computing services upon presentation of departmental employment verification. Some services require the presentatio

					n of a valid UNT id.
UNT fulltime/part-time faculty and staff - Health Science Center	Payroll Office	as per interagency agreement	as per interagency agreement		
UNT fulltime/part-time faculty and staff - Universities' Center at Dallas	Payroll Office	yes	yes		
UNT Retired Faculty and Staff and unmarried surviving spouses	Human Resources	yes	yes		
Visiting Scholars not on payroll	associated department	yes - as appropriate	yes - as appropriate	length of visit	Authorization procedure is required
Guest Workshop Faculty and Staff	associated department	yes - as appropriate	yes - as appropriate	length of visit	Authorization procedure is required
Consultants under contract with UNT units	associated department	no	yes	contract length	Authorization procedure is required
Board of Regents members		yes	yes	length of tenure	
Continuing Education Faculty	Continuing Education Office	contracted	contracted		
People and Programs - Miscellaneous					
Community users (pre-college, other citizens)		no	Community users may access the central web portal as guests		
Affiliated non-profit organizations and institutes		contracted	contracted	length of affiliation/contract	
Affiliated commercial organizations and institutes		contracted	contracted	length of affiliation/contract	

Community organizations		contracted	contracted	length of affiliation/contract	
Visiting Evaluators and State Auditors	State of Texas	yes	yes	length of task	Services granted as task requires and in keeping with state laws and guidelines and this policy
Other Texas states institutions/affiliates students, faculty, and staff		no	no		
Spouses/Partners/Children/Parents of UNT authorized users		no	no		The sharing of remote access accounts by immediate family members residing in the same household is allowed. The UNT authorized user is ultimately responsible for the security of his or her account
Note: Other remote access accounts, for the benefit the University, may be approved on an individual basis by the Associate Vice President for Computing and Chief Technology Officer.					

VII. Potential Liability for Failure to Adhere to this Policy. It is important to note that failure to adhere to this Policy may lead to the cancellation of a user's computer account(s), suspension, dismissal, or other disciplinary action by the University, as well

as referral to legal and law enforcement agencies. The following are some laws that pertain to computer usage:

A. Texas Administrative Code, 1 TAC §202C: Information Security Standards. State of Texas law that sets forth the requirements state entities must follow regarding computer security.

B. Texas Penal Code, Chapter 33: Computer Crimes. State of Texas law specifically pertaining to computer crimes. Among other requirements, unauthorized use of University computers or unauthorized access to stored data, or dissemination of passwords or other confidential information to gain access to the University's computer system or data is in violation of criminal law.

C. Texas Penal Code, Chapter 37: Tampering with Governmental Record. Any alteration, destruction, or false entry of data that impairs the validity, legibility or availability of any record maintained by the University is a violation of criminal law.

D. United States Penal Code, Title 18, Chapter 47 - Fraud and False Statements, Section 1030: Fraud and related activity in connection with computers. Federal law specifically pertaining to computer crimes. Among other requirements, prohibits unauthorized and fraudulent access.

E. Computer Fraud and Abuse Act of 1986. Part of Title 18, Chapter 47, Section 1030. Makes it a crime to access a computer to obtain restricted information without authorization; to alter, damage, or destroy information on a government computer; and to traffic in passwords or similar information used to gain unauthorized access to a government computer.

F. The Computer Abuse Amendments Act of 1994. Part of Title 18, Chapter 47, Section 1030. Expands the Computer Fraud and Abuse Act of 1986 to address the transmission of viruses and other harmful code.

G. Federal Copyright Law. Recognizes that all intellectual works are automatically covered by copyright. The owner of a copyright holds the exclusive right to reproduce and distribute the work.

H. Digital Millennium Copyright Act. Signed into law on October 20, 1998 as Public Law 105-304. Created to address the digitally networked environment, the DMCA implements the WIPO Internet Treaties; establishes safe harbors for online service providers; permits temporary copies of programs during the performance of computer maintenance; and makes miscellaneous amendments to the Copyright Act, including amendments which facilitate Internet broadcasting.

   For further clarification of the DMCA refer to the Digital Millennium Copyright Act Summary and the Fair Use Factsheet.

I. Electronic Communications Privacy Act of 1986. Prohibits the interception or disclosure of electronic communication and defines those situations in which disclosure is legal.

J. Computer Software Rental Amendments Act of 1990. Deals with the unauthorized rental, lease, or lending of copyrighted software.

Responsible Party. Computing and Information Technology Center

References and Cross-references.

Texas Administrative Code, 1 TAC §202C: Information Security Standards
Texas Penal Code, Chapter 33: Computer Crimes
Texas Penal Code, Chapter 37: Tampering with Governmental Record
United States Penal Code, Title 18, Chapter 47 - Fraud and False Statements, Section 1030: Fraud and related activity in connection with computers
Computer Fraud and Abuse Act of 1986
The Computer Abuse Amendments Act of 1994
Federal Copyright Law
Digital Millennium Copyright Act
Electronic Communications Privacy Act of 1986
Computer Software Rental Amendments Act of 1990

Approved: 8/1/1997
Revised: 8/01; 11/05; 7/11*
*Format only