OIS 42 – Standard for Acceptable Use

I. STANDARD STATEMENT

All personnel seeking to access UTSA computing resources must be aware of the duties and responsibilities that are in place to protect the network infrastructure. This document may also be called the Acceptable Use Policy (AUP).

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

informationsecurity@utsa.edu

V. DEFINITIONS

A. **appropriate network server -** A computer asset meeting the minimum setup criteria: authentication, data protection, server administrator assigned. (April 2013)
B. critical University digital data - Generally, data that is defined by an entity to be essential to that entity's function and that, if made unavailable, will inflict substantial harm to the entity and the entity's ability to meet its instructional, research, patient care or public service missions.
C. **Executive Officer** - UTSA President (or delegate), UTSA Provost (or delegate) (April 2013)
D. **excessively large (email) message or attachments** - The maximum size for a UTSA email message is 20MB, including the message and all attachments.
E. **incidental use** - certain activities (accessing the Internet, installing software like iTunes, etc.) are permitted as long as they do not affect the execution of your work duties and they do not incur an expense or hardship to the university. For example, maxing out your computer hard drive space with your personal files is not permitted.
F. **Chief Information Security Officer or his/her delegate** - The delegates consist of the UTSA President, Provost or delegate of the Provost.

VI. PROCEDURES

A. All faculty and staff members seeking to access UTSA information resources must be aware of the duties and responsibilities that are in place to protect the university network.

B. Acknowledgement of Acceptable Use Policy
Each User, during the normal compliance training process, reviews and acknowledges their understanding and acceptance of the Acceptable Use Policy.

C. General
1. UTSA Information Resources are provided for the express purpose of conducting the business and mission of the UTSA.
2. UTSA Information Resources must not be used to: engage in acts against the mission and purposes of the UTSA, intimidate or harass, degrade performance, deprive access to a UTSA resource, obtain extra resources beyond those allocated, or to circumvent computer security measures.
3. Information Resources must not be used to conduct a personal business or for the exclusive benefit of individuals or organizations that are not part of The University of Texas System.
4. Sexually explicit materials must not be intentionally accessed, created, stored or transmitted other than in the course of academic research where this aspect of the research has the explicit written approval of an Executive Officer of UTSA.
5. Users must not copy or reproduce any licensed software unless expressly permitted by the software license, use unauthorized copies on UTSA-owned computers or use software known to cause problems on UTSA-owned computers.

D. Information Services Privacy
1. Users have no expectation of privacy regarding any data residing on UTSA computers, servers, or other Information Resources owned or held on behalf of UTSA regardless of whether the data was generated as the result of acceptable (including Incidental Use as described below) or unacceptable use of UTSA's Information Resources.
2. All files, documents, messages in any format and other data residing on UTSA computing resources or held on behalf of UTSA are accessible to UTSA in accordance with the Regents' Rules and Regulations and are subject to access by the UTSA without notice to comply with public information requests, court orders, subpoenas or litigation holds; or for any other purpose consistent with the duties of UTSA. Users have no expectation of privacy in any such data.

E. Data Protection
1. Data will be accessed on a need to know basis. Users of UTSA Information Systems must not attempt to access data or programs contained on systems for which they do not have authorization or consent.
2. All critical University digital data will be saved on appropriate network servers to ensure backup of the data. All data, including research data, should be backed up for disaster recovery reasons.

3. All records (electronic or paper) will be maintained in accordance with the UTSA Records Retention Policy.

F. Electronic Mail (email)
   1. The email service provided by the university (@utsa.edu domain) is the official university email system for employees. Employees of UTSA shall not use other email services for UTSA business. The following email activities are prohibited:
      a. Using email for purposes of political lobbying or campaigning except as permitted by the Regents' Rules and Regulations.
      b. Posing as anyone other than oneself when sending email, except when authorized to do so by the owner of the email account.
      c. Reading another User's email unless authorized to do so by the owner of the email account, or as authorized by policy for investigation, or as necessary to maintain services.
      d. Use of email software that poses a significant security risk to other Users on the UTSA network.
      e. Sending or forwarding "chain" letters.
      f. Sending unsolicited messages to large groups except as required to conduct UTSA business.
      g. Sending excessively large messages or attachments unless in performance of official UTSA business.
      h. Sending or forwarding email that is likely to contain computer viruses.

G. Confidential or Protected Information (Category I / II data)
   1. Users shall not disclose confidential information except to authorized parties as required to accomplish authorized business functions in support of UTSA's mission.
   2. All confidential or protected health or student information transmitted over external networks or saved on UTSA servers must be encrypted in accordance with university data encryption guidelines. This information must not be sent or forwarded to non-UTSA email accounts provided by other Internet Service Providers, and must not be knowingly transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols and security techniques are utilized.
   3. A link to more information about data classification can be found on the Data Classification Examples page.

H. Incidental Use of Information Resources
   1. Incidental personal use of email, Internet access and other Information Resources by an employee is permitted by UTSA policy but is restricted to employees (it does not extend to family members or other acquaintances). It must not interfere with the normal performance of an employee's duties, must not result in direct costs to UTSA and must not expose the University to unnecessary risks.
   2. Non-work related information may not be stored on network file servers.

I. Internet Use

1. Due to network maintenance and performance monitoring and to ensure compliance with applicable laws and policies, all User activity may be subject to logging and review.
2. Email or postings by Users of UTSA network resources to news groups, "chat rooms", "listservs", or social websites must not give the impression they are representing, giving opinions, or making statements on behalf of UTSA, unless authorized. Users should use a disclaimer stating that the opinions expressed are their own and not necessarily those of UTSA.
3. Personal commercial advertising must not be posted on UTSA websites.

J. Security

Security programs or utilities that reveal or exploit weaknesses in the security of a system or that reveal data by circumventing established authorization procedures and systems should not be downloaded and/or used, except as authorized by the Office of Information Security (OIS). Users must report any identified weaknesses in UTSA computer security and any incidents of possible misuse or violation of this Acceptable Use Policy to an immediate supervisor, department head or OIS.

K. Exceptions

Any exceptions to this Acceptable Use Policy must be documented and authorized in writing by the CISO or his/her delegate.

Title: OIS-42 Standard for Acceptable Use
Effective Date: September 4, 2014
Last Reviewed: August 12, 2020