OIS 46 – Standard for Information Resources User

I. STANDARD STATEMENT

This standard addresses the expectation of privacy with respect to the use of UTSA information resources.

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. GENERAL

A. Internal UTSA users (including faculty, staff, students, contractors and others) should have no expectation of privacy with respect to the use of information resources, except as provided in the Regents Rules and Regulations of the University of Texas System. Electronic files created, sent, received or stored on computers and other information owned, leased, administered, or otherwise under the custody and control of UTSA, are not private. They may be accessed as needed for purposes of system administration and maintenance, for resolution of technical problems, for compliance with the Texas Public Information Act, subpoena, or court order and to perform audits.

B. Third parties have entrusted their information to UTSA for business, learning and professional purposes. All users must do their best to safeguard the privacy and security of this information. The most important of these third parties is the individual student. Student account data, protected health information and educational record data are confidential, and access will be strictly limited based on a business need for access.

C. To manage systems and to enforce security, University Technology Services (UTS) may log, review and otherwise utilize any information stored on or passing through the university's information systems in accordance with the provisions and safeguards provided in the First Article of Texas Administrative Code, Section 202, parts 1-8, Information Resource Standards.

D. In suspected cases of abuse of information resources, the contents of any e-mail or file may be reviewed in accordance with provisions defined in the Disciplinary Actions section of the Information Resources Use and Security Policy.

E. All university-owned computer desktops must remain "on," including during overnight hours. Critical patches are usually pushed over the network to individual workstations after regular duty hours. UTS acknowledges that this is not a "green" solution, but in this instance, the information security risk is more important. Other peripherals (monitors, etc.) may be shut off. NOTE: The automatic update process may require a desktop computer to be rebooted on the next log in attempt.

IV. PROCEDURES

A. General
   1. UTSA information resources are provided for the express purpose of conducting the business and mission of the University.
   2. All users of UTSA information resources must be familiar with and be in compliance with the UTSA Acceptable Use Policy.

B. Passwords and Passphrases
   1. Any password/passphrase used to access UTSA data must, at minimum, meet the requirements set forth in the Standard for Password/Passphrase. This includes the accessing of UTSA data stored on services outside of the university.
   2. Users must take special care to secure their passphrase and are prohibited from disclosing the passphrase to any person or entity.
   3. If a user knows or suspects that a password or passphrase used to access university resources has been compromised, the password or passphrase must be changed as soon as possible.
   4. Faculty and staff members are expressly forbidden from sharing any password or passphrase that is used to access university information resources.

C. Information Resources Security
   1. UTSA is committed to academic freedom, regardless of the medium of expression. However, in order to provide the optimum use of its information resources for the entire university community:
      a. UTSA reserves the right to limit or restrict use based on institutional policies and financial considerations, as well as in the event of a violation of university policy, contractual agreement or state/federal laws.

b. The individual's rights of expression or privacy may be superseded by the responsibility of the university to protect the integrity of information technology resources, the rights of all users and property of the university.

2. Both the university community as a whole and each individual user have an obligation to abide by the published standards and best practices of the information security program, as discussed in this policy and in the published standards. Protecting the integrity of UTSA's shared information resources and preserving access to them is a community effort that requires each individual user to:
   a. Act responsibly.
   b. Guard against abuses.
   c. Be responsible for the resources assigned to them and to follow good judgment in the protection of those resources. The InSight application contains a variety of resource management tools to help maintain and manage your resources.
   d. Abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.
   e. Inappropriate activities include, but are not limited to:
      i. Identity Theft
      ii. Intentionally accessing or attempting to access unauthorized information
      iii. Downloading copyrighted material without proper authorization
      iv. Operating an outside business using university resources
      v. Using UTSA information resources for fraudulent or illegal activities
3. Computer equipment and devices accessing UTSA information resources
   a. University-owned computer
      i. Must meet requirements as set forth in the InSight application, as described in this Standard.
      ii. Must use the computer naming convention as described in the Standard for Computer Naming Convention.
      iii. Data that only exists on the computer should be backed up on a regular basis. For more information on the preferred software solution, see the Data Backup page.
      iv. If the computer is taken off campus, a Removal of Equipment form must be completed and approved.
      v. Users authorized to access computer applications must abide by the requirements of the log-in disclaimer, as specified in the Standard for Log-in Disclaimer Text.
      vi. Most university-owned computers must be encrypted, unless they are exempted from this requirement. Note that computers purchased

before September 1 are not required to be encrypted unless they store Category I data. Exemptions are granted by the UTSA Office of Information Security.

vii. If the computer is not part of the UTSA domain, the user is responsible for ensuring that all operating system patches and updates are installed in a timely manner.

viii. All university-owned computing devices must be disposed of in the manner set forth by the UTSA Surplus department.

b. Personally-owned computer used to access university resources

i. Personally-owned computers used to access university resources or conduct university-related business must be configured with equivalent security options as would be required on a university-owned resource storing similar data or performing similar functions.

ii. Before a computing device that contained UTSA data is sold, transferred or returned, the user must render the data unreadable.

iii. Mobile device (university- or personally-owned) used to access university resources

iv. Device must be protected by a PIN or other protection method native to the device.

v. Device should be encrypted.

vi. Device should have remote wipe (reset) enabled, if that feature is available.

vii. Before a mobile device that contained UTSA data is sold, transferred or returned, the user must ensure that all of the data has been deleted.

D. Software

1. Licensed software cannot be copied or reproduced, except as expressly permitted by the software license.
2. Unauthorized software cannot be used or installed on University-owned computers and devices.
3. Software known to cause problems cannot be used or installed on University-owned computers and devices.
4. Faculty and staff members must be able to produce valid licenses for all software installed on their machines.

E. Data Protection

1. Users must protect data in the manner appropriate for its classification, as specified in the Standard for Data Classification Guidelines.
   a. University data cannot be saved on services that are not managed nor affiliated with UTSA through an existing contract.
   b. Any university data that is stored in an offsite location must be secured as per the requirements stated in the Standard for Enterprise Backup and Data Recovery.
      i. Devices used to store data in transit must be encrypted in accordance with current industry standards.

ii. External devices (USB flash drive, USB hard drive, etc.) used to store Level I or Level II data must utilize hardware encryption features, including a Personal Identification Number (PIN) or password/passphrase.

F. Email
   1. Other than in times of emergency, all faculty/staff university business conducted via email must be conducted using official UTSA email accounts.
   2. University-issued email accounts for faculty and staff cannot be used for commercial purposes.
   3. Faculty and staff members are not permitted to auto-forward UTSA email to a personal email account.

G. Network and Remote Access
   1. Users who have a need to securely access university network resources from a remote location must connect using the UTSA Virtual Private Network (VPN) or other approved methods.
   2. Connecting to the UTSA network using a third-party software product (LogMeIn, GoToMyPC, etc.) is forbidden, unless the connection is initiated through the UTSA Virtual Private Network (VPN).
   3. Students, faculty and staff members are prohibited from setting up personal Access Points, unless expressly authorized by the Office of Information Security.

H. Policy Review

In order to maintain currency of the Information Security Program, this policy is subject to review on a regular basis.

I. Policy Violation
   1. Violation of this policy and its standards may result in disciplinary action for permanent and/or temporary employees through regular, published disciplinary procedures, including:
      a. Termination of employment
      b. Termination of employment relations, in the case of contractors or consultants
      c. Dismissal, for interns and volunteers
      d. Suspension or expulsion of students
         i. If no other documented disciplinary procedures are in place
         ii. Disciplinary action for a faculty member will be referred to the faculty member's department, dean and the Office of the Provost.
         iii. Disciplinary actions for staff will be referred to the staff member's supervisor through the vice president of the division where the staff member is employed.

2. In addition to the potential disciplinary actions stated above, individuals may lose access to UTSA information resources and may face civil and/or criminal penalties, depending on the severity of the violation(s).

Title: OIS 46 – Standard for Information Resources User
Effective Date: September 4, 2014
Last Reviewed: August 12, 2020