UTSA Institutional Compliance Office of Information Security

OIS 52 – Data Security while Telecommuting

I. STANDARD STATEMENT

The purpose of this standard is to assist managers and employees to ensure the safety and confidentiality of University of Texas at San Antonio (UTSA) data and systems by adhering to sound computing practices and UTSA's information security requirements for telecommuting arrangements. This document identifies the security requirements and the parties responsible for implementation and/or ongoing adherence to those requirements.

II. RATIONALE

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

III. SCOPE

This standard applies to all UTSA faculty and staff who are telecommuting. Telecommuting is defined as work done off-campus.

IV. CONTACTS

Informationsecurity@utsa.edu

V. Administrative Requirements

It is the responsibility of school and business unit leadership (e.g. deans, department chairs, managers, supervisors) to ensure adherence with the following requirements for all individuals within the school or business unit who participate in telecommuting arrangements.

A. General

1. All telecommuting arrangements must be approved and documented by the user's manager or unit leadership.

2. Only institutionally owned and supported computers that meet the requirements specified within this standard may be used for telecommuting arrangements.

B. Technical

1. General Security Requirements

   a. All computers must be encrypted
   b. All systems used to telecommute must be kept up-to-date with the most current security patches for the operating system as well as any applications such as Anti-virus software, Microsoft Office, Internet Explorer, Firefox, etc.
   c. Only operating systems and applications currently supported by the UTSA are allowed.
   d. Computer systems must have System Center Configuration Manager (SCCM) or Absolute Manage (AM) client installed to ensure UTSA computer assets are tracked, receiving the necessary and required computer updates and anti-virus/anti-malware updates
   e. All computers must connect and backup the computer local drive (user profile) data using the CrashPlan desktop application.

2. Anti-Virus Requirements

   a. All systems used to telecommute must have anti-virus software installed and properly configured.
   b. The anti-virus software must be kept up-to-date with the most current signatures and scan engines, and be configured to automatically retrieve and apply updates on a daily basis.

3. Printing

   No printing of UTSA data will be allowed by telecommuters.

4. Network Security Requirements

   a. All systems used to telecommute must be protected with a firewall.
   b. The firewall may be either hardware or software based
   c. The firewall must be configured to block all unsolicited inbound connections.

5. Authentication/Authorization Requirements

   a. All systems used to telecommute must require users to login before using the system.
   b. Administrative rights should be restricted to local IT staff. Telecommuters should not be given administrative authority to the computer used for telecommuting.

6. Security Incident Reporting Requirements

   a. If a system used to telecommute is lost, stolen, compromised, or suspected of being compromised, the user must immediately report the incident to their manager and OIT Connect. OIT Connect is responsible for reporting the incident to the Office

of Information Security (OIS).

VI. User Requirements

A. It is the responsibility of individuals who participate in telecommuting arrangements to ensure their adherence with the following requirements.

B. General Security

Users must not attempt to bypass computer security measures or modify security configuration settings.

C. Network Security

1. Only the following network connectivity methods may be utilized for telecommuting arrangements:

   a. Preferred is to connect to a wired network and utilize the UTSA's VPN.
   b. If wired not available, wireless is acceptable if is in configured by WPA2 or higher.

2. Authentication

   a. Users will use two-factor authentication (DUO) when logging into the UTSA network.
   b. Note: Access to some applications may require a second two-factor authentication.

3. Data categorization
   a. Category 1 data – data whose disclosure, destruction, display, or modification would violate state of federal laws or regulations, UT System policies or the Texas Open Records Act.
   b. Category 2 data – data not otherwise protected identified as *confidential* data, but which are releasable with the Texas Public Information Act. Data protected to ensure a controlled release.
   c. Category 3 data – University data that have no requirement for confidentiality, integrity, or availability. Published (aka Public) data, while subject to UTSA disclosure rules, is available to the UTSA community and all external individuals and entities.

4. Category 1 or some Category 2 data includes but is not limited to:
   a. Social Security Numbers,
   b. Government issued ID numbers (e.g. Driver's license number),
   c. financial account numbers (e.g. bank accounts, credit card accounts),
   d. Data protected under FERPA (e.g. student grades),
   e. Data entrusted to UTSA by governmental entities (e.g. Veterans Administration, NIH) or other parties on the condition that the data be adequately protected.
   f. Personally Identifiable Information
   g. Medical information
   h. Users must not store Category 1 or Category 2 data on any system used for telecommuting unless authorized by OIS. If authorized by OIS, such should consist of the absolute minimum necessary information required to perform the job. The "i:" and "s:" drives are

the primary storage locations for all Category 1 and category 2 data.

i. Users must never allow unauthorized individuals to access Category 1 or Category 2 data or use the system issued to them that is specified for the telecommuting arrangement.
j. Users must not store Category 1 or Category 2 data on non-UTSA owned systems or removable media (CD's, USB hard drives, flash drives, etc.)
k. While workflows may need to allow for Category 1 or Category 2 data to be viewed, this data that is no longer needed must be promptly deleted from the system as per records retention policies.
l. Any system or removable media used to store Category 1 or Category 2 data must be disposed of in a manner that renders any sensitive data on the device/media unrecoverable. Examples include physical shredding, logical disk wiping, and degaussing.
m. Systems must be returned to UTSA when the telecommuting arrangement is ended.

5. Security Incident Reporting

a. If a system used to telecommute is lost, stolen, compromised, or suspected of being compromised, the user must immediately report the incident to their manager and OIT Connect.
b. Any system used to telecommute must be made available upon request by OIS for examination in order to respond to actual or suspected security incidents.

7. Compliance

Users who access Category 1 or Category 2 data that is protected by regulation (e.g. HIPAA, FERPA) or contract (e.g. credit card data) must comply with any additional requirements dictated by the governing regulations/contracts

Title: OIS 52 – Data Security while Telecommuting
Effective date: October 7, 2010
Last Reviewed: August 10, 2020