Standard for Secure Office Suites

Objective

In accordance with the Information Security and Acceptable Use Policy, Confidential Data must be protected from accidental disclosure. Offices that routinely handle Confidential Data may benefit from additional security precautions consistent with the value of the data to be protected.

Perimeter Security

When possible, office suites should have a secure perimeter. If general access is required, then a configuration of a single door with a staffed reception desk is recommended. Card readers should be used to restrict access on doors intended for use by authorized staff only. Video cameras may also be used to provide accountability of who enters and exits the suite. Doors must be kept locked when the office suite is not staffed.

Office suites determined to be high-risk by the UT Dallas Police Department may be equipped with silent alarm panic buttons.

Guests

Guests should not be granted access to UT Dallas Information Systems without proper authorization. If a guest requires access to UT Dallas Information Systems, please refer to the Guest Access Security Standard.

UT Dallas Information Systems should not be shared with guests who have not been provided with UT Dallas NetID accounts. Rather, guests should be encouraged to use their own computers and connect to the “UTDGuest” wireless network when Internet access is needed. Departments may also provide loaner laptops for guest use, provided that loaner laptops are routinely scrubbed of all data.

When useful, guests may be required to sign an access log at a receptionist station and may be provided with badges identifying them as guests. This is intended to help employees identify when a person is present who may have fewer rights to protected information. In cases where especially high-risk information is handled, visitors may need to be escorted.

Clean Desk Initiatives

Departments may require employees follow a “Clean Desk” procedure, to prevent inadvertent disclosure of Confidential Data. Some examples include:

- Laptops and portable media devices should be locked away when not in use.
- Employees should remove confidential paper files and secure them in appropriate locations when not in use or when the Employee is not present.

- Employees should be trained to turn over or conceal paper documents containing Confidential Data when guests are present.
- Employees must lock their computers with password-protected screen saver functions when away from their desks.
- Computer monitors should be located so as to limit the ability for individuals outside the suite to view them – for example, monitors should not face an open door or window. When needed, privacy screens may be used on computer monitors to limit this possibility.
- Users should not display written passwords in their work space where others could observe such passwords.

Printers and Copiers

Printers and copiers should be located in areas not frequented by the general public. If HIPAA-protected or other high-risk data is printed, the printer should be located in a room with access restricted to authorized personnel. Departments may opt to require employees to enter a passcode at the printer before a print job is completed.

Shredders and Recycle Bins

In order to appropriately dispose of Confidential Data, office suites where it is routinely handled should have either a shredder or locked recycling bin, consistent with the Data Storage and Disposal Standard.

Exemptions

In the event that compliance with this standard cannot be met, please contact infosecurity@utdallas.edu to discuss alternatives and options.