Securing Publicly Accessible Devices

Responsible Officer: Vice President for Office of Information Technology
Sponsoring Department: Office of Information Technology
Revision Date: 16 March 2015
Errors or changes to: aim@uta.edu

CONTENTS

PROCEDURE OBJECTIVE

Provide a procedure for securing publicly accessible computers to ensure that these devices will not be used to gain unauthorized access to the University information resources. This procedure supports *Administrative Office Roles and Responsibilities for Information Resources* (Policy 5-603).

SCOPE

This procedure addresses the protection of desktop, laptop, and tablet devices that are publicly accessible through the restriction of physical and end-user access and provision of data protection.

RESPONSIBILITIES

Office of Information Technology

- Provide tools that protect data (data erasing or encryption tools).

- Provide network authentication methods.
- Provide an exception process for machines that are unable to meet guidelines in Sections I, II, and III.
- Monitor compliance of safeguards for machines that received exceptions.
- The Vice President of Information Technology will resolve any questions related to this procedure.

Academic and Administrative Offices

- Ensure that all publicly accessible computers are following procedures outlined in Sections I, II, and III or that an exception has been filed for those devices that are unable to meet guidelines.

PROCEDURES

Section I. Physical Protection of Publicly Accessible Devices (Desktops, Laptops, and Tablets)

A. Department heads will ensure that all deployed devices have a UTA asset tag.

B. The department IT staff will acquire and apply a cabling and lock mechanism or other secure mounting device in order to physically lock all desktop computers.

1. IT Compliance (itcompliance@uta.edu) will provide assistance in identifying and implementing a solution if needed.

C. Department staff will verify client identity by checking the UT Arlington MavExpress card prior to loaning mobile devices such as laptops and tablets to members of the campus community.

D. Department IT staff will request an exception for all devices that cannot be physically secured as documented in Section I using the process in Section IV.

Section II. Limit Unauthenticated Access to Publicly Accessible Devices

A. Department IT staff will utilize centrally provided network authentication methods to enable tracking of individual users of the machine if supported by the business function of the device.

B. Department IT staff will request an exception as designated in Section IV for all devices that do not support network authentication due to business function and ensure that the device can be used for no other function than the business process (such as a kiosk).

Section III. Data Protection on Publicly Accessible Devices

A. Department IT staff must utilize currently accepted encryption methods on all devices that are required to be encrypted. Acceptable methods are documented at http://www.uta.edu/security/encryption/fulldiskencryption/index.php.

B. Department IT staff must request an exception for all publicly accessible devices that cannot be encrypted without limiting their business function as designated in Section IV.

Section IV. Exceptions

A. If a device cannot meet the guidelines outlined Section I or II, then the department IT staff should request an exception by emailing itcompliance@uta.edu with the following information in an Excel format:

1. Email itcompliance@uta.edu with the following information (Excel worksheet):

    a. Asset tag number(s)

    b. Serial number(s)

    c. Device location

    d. Method(s) of physical protection (in cases where Section I protections are not possible)

    e. Method(s) of limiting access to device outside of designed business function (in cases where Section II protections are not possible)

B. If a device cannot meet the guidelines outlined in Section III, then the department IT staff should request an exception using the process below:

1. Department IT staff will ensure that data cannot be saved to the publicly accessible device. Centrally provided tools (such as DeepFreeze) must be used.

2. Submit *Computing Device Encryption Exception Request* (Form 18-1) to security@uta.edu or fax to 817-272-2612 with an Excel file that includes the asset tags, serial numbers, and computer names of devices.

FORMS AND TOOLS/ONLINE PROCESSES

Computing Device Encryption Exception Request (Form 18-1)

Encryption Standards

DEFINITIONS

Desktop Computers: Devices such as desktops computers that would reasonably be considered stationary and not portable.

Mobile Computers: Devices such as laptops and tablet computers that are reasonably considered portable.

Publicly accessible devices: Kiosks, walk-up computer stations, or other devices that are readily available to the public because they are not protected by reasonable means such as physical restrictions (room lock, card swipe, or access attendants), electronic restrictions (authenticated access), and/or a identity verification process before the distribution of an asset (loaner laptops).

RATIONALE

The intent of this procedure is to ensure that publicly accessible devices will not be used to gain unauthorized access to the University information resources.

RELATED STATUTES, POLICIES, REQUIREMENTS OR STANDARDS

UT System Administration Policies and Standards	Other Policies and Standards
N/A	*Administrative Office Roles and Responsibilities for Information Resources Policy* (Policy 5-603).

APPENDICES

N/A

CONTACTS

If you have any questions about this procedure, contact the following departments:

Subject	Office Name	Telephone Number	Email/URL
All topics in procedure	Office of Information Technology	817-272-5519	cio@uta.edu
Website access	Administrative Information Management	817-272-0222	aim@uta.edu http://www.uta.edu/aim

WEBSITE ADDRESS FOR THIS PROCEDURE

https://www.uta.edu/policy/procedure/19-3