Kiosk Security Standard

1. Purpose

This standard was created to set minimum requirements for generally shared devices that need to be easily accessible for faculty, staff, students, and the general public, which adhere to current security best practices and drafted in response to UTS-165, necessary to create a safe computing environment. Compliance with this standard will increase the level of security for kiosks in order to better protect University Information Resources. These minimum requirements exist in addition to all other UTRGV policies and federal and state regulations governing the protection of UTRGV's data.

2. Scope

This standard applies to:

a. All computing devices owned, leased or managed by UTRGV that are generally shared and easily accessible by faculty, staff, students, and the general public

This standard does not apply to:

a. UTRGV owned, leased or managed computers that fall within the regular UTRGV Computer Security Standard

3. Audience

All employees, students, consultants, vendors, contractors, other affiliated and non-affiliated persons, who operate a computing device within the defined scope,

4. Authority

UTS 165, UTRGV AUP

5. Definitions

Computer – Includes but is not limited to all computing devices (physical or virtual) such as desktops, workstations, servers, laptops, tablets, and smart phones

Kiosk – An interactive computing device that is easily accessible

Personally Owned – Includes any computer which is not owned, leased or managed by UTRGV

Portable Computer – Includes any computer which is portable and typically runs on batteries such as but not limited to laptops, tablets, and smart phones

Software Firewall – Software that limits network traffic to and from a computer based on a security policy

6. Standard Details

6.1. Requirements for all computers

6.1.1 Operating system and application security update and/or patches should be expediently installed

6.1.1.1 Configuration changes should be performed in a manner consistent with change management procedures

6.1.2 Computer hostnames must adhere to the UTRGV Computer Naming Standard and include the asset property number at the end

6.1.3 Domain Membership

6.1.3.1 Kiosk computers must be joined to the UTRGV Domain under the Kiosk Group (OU)

6.1.3.2 Only UTRGV owned, leased, or managed computers may be joined to the UTRGV domain

6.1.4 Administrative privileges

6.1.4.1 The built-in local administrator account must be disabled and renamed

6.1.4.2 For UTRGV domain joined computers, LAPS must be used to properly manage enabled local administrator accounts in order to enforce password policies, standards and best practices

6.1.4.3 Logging on with administrative privileges should be limited for activities that require it and for the duration of the activity

6.1.4.4 Administrative privileges are limited to certain employees who are responsible for providing administrative services such as system maintenance and user support

6.1.4.5 Requests for local administrative privileges will be granted following an approval process defined by the Information Security Office

6.1.5 Products, including operating systems, that no longer receive security updates from the vendor (e.g., unsupported) are not authorized

6.1.6 Must have a software firewall that is enabled and managed by UTRGV Computer Support Staff

6.1.6.1 Must have enabled malware protection (antivirus) software with up-to-date definitions

6.1.6.2 Must be free of malware and not using software in a manner that infringes on copyright laws

6.1.7 All kiosk computers must be physically secured

6.1.8 Must be encrypted and password protected using methods approved by the UTRGV Information Security Office

6.1.8.1 The use of full disk encryption is required

6.1.8.2 Default and generic usernames and passwords should be changed or disabled

6.1.9 Computer must be set for auto logon

6.1.9.1 Password should not be shared outside IT

6.1.9.2 Please use the UTRGV kiosk account for auto login (SVR_KIOSK)

6.1.10 Screen Lockout

6.1.10.1 Screen lockout will not be required

6.1.11 The device or computer should be capable of returning to a preconfigured state

6.1.11.1 System must be configured such that no information is permanently saved on system upon system restart or user log-out

6.3.11.2 Kiosks should be configured to reset to a standard image after a reasonable amount of time when not in use

6.1.12 Computer backups

6.1.12.1 Computer backups are the responsibility of the computer operator or primary user

6.1.13 Computers must have auditing tools installed that allows the Information Security Office to validate that the computer is compliant with UTRGV, UT System, state and federal policies and standards.

7. Roles and Responsibilities

7.1 **Resource Owner**: Ensures that the any kiosk which they own or operate meets all the requirements of this security standard. Engage with UTRGV Computer Support Staff for guidance and compliance with this standard.

7.2 **UTRGV Computer Support Staff**: Ensure that all computers are configured to support the requirements defined in this standard.

7.3 **Information Security Office**: Define and maintain this standard to a level that can define the necessary configurations and security practices to protect UTRGV information resources and ensure compliance with all UT System, state and federal policies and standards

8. Non-Compliance and Exceptions

8.1 For individuals with administrator access—if any of the requirements contained within this standard cannot be met on applicable information resources you use or support, the Security Exception Process must be followed to address any associated risk

8.2 Machines defined by Kiosks by the Information Security Office which do not adhere to this standard, may lose access to UTRGV resources

8.3 Non-compliance with this standard may result in notification of supervisors, and may be subject to disciplinary action in accordance with applicable UTRGV rules and policies

9. Related Policies, Standards and Guidelines

UTS 165
UTRGV AUP
UTRGV Data Classification Standard
UTRGV Computer Naming Standard
UTRGV Security Exception Standard
NIST 800-53 Revision 4
Center for Internet Security (CIS) Critical Security Controls Version 6

Appendix

I. Examples

- Kiosk machines used for non-affiliated students
- Sign-in tablets:
  - Sign-in station for prospective or current employees
  - IPads where international (current, or future) students can sign-in when visiting the International Admissions and Student Services Office
  - Tablets in the UTRGV Student Food Pantry where users can sign-in