Computer Security Standard

1. Purpose

This standard was created to set minimum requirements, 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 computers 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 computers owned, leased or managed by UTRGV
b) Any computer (physical or virtual) connecting to a UTRGV network through wired, wireless, or VPN connection
c) Any computer which stores or accesses UTRGV confidential or sensitive data.

3. Audience

All employees, students, consultants, vendors, contractors, and others who operate a computer 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.

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

Portable Computer – includes any computer that 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.

Computer Lab – Set of computers in close proximity which provides services to a UTRGV defined group.

Podium Computer – UTRGV computing device located in a room for presentations/lecture.

6. Standard Details

6.1 Requirements for all computers

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

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

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

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

6.1.5 Must be password protected

6.1.5.1 Default and generic usernames and passwords should be changed or disabled.

6.1.6. Users must log out or lock computers when leaving them unattended

6.1.7. The use of a software firewall is required

6.1.8 The use of full disk encryption is required

6.1.9 Computer backups

6.1.9.1 Computer backups are the responsibility of the computer operator or primary user.

6.2. Additional requirements for all computers owned, leased or managed by UTRGV

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

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

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

6.2.4 Unattended Computer Security

6.2.4.1 Screen Lockout

6.2.4.1.1 All computers must be configured to auto-lock and be password protected after a maximum of 20 minutes of inactivity

6.2.4.2 Unattended portable computers must be physically secured

6.2.5 Computer hostnames must adhere to the UTRGV Computer Naming Standard

6.2.6 Domain Membership

6.2.6.1 Wherever possible, computers must be joined to the UTRGV domain, unless granted an exception by the Information Security Office

6.2.6.2 When joined to the UTRGV domain, local accounts must not exist

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

6.2.7 Administrative privileges

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

6.2.7.1.1 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

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

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

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

6.2.8 Computers which store UTRGV confidential data must be registered with the Information Security Office

6.3 Additional requirements for all computers, including personally owned computers, that store or access UTRGV confidential or sensitive data. (Please refer to the UTRGV Data Classification Standard for guidance with Data Classifications.)

6.3.1 Must be password protected using standards approved by the UTRGV Information Security Office

6.3.2 Any computer on which Confidential University Data is stored or created must be encrypted using methods approved by the UTRGV Information Security Office

6.3.3 Backups should only be stored on UTRGV owned or sanctioned storage and must be encrypted and password protected

6.3.4 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. Additional requirements for all Lab and Podium computers owned, leased or managed by UTRGV

7.1 Domain Membership

7.1.1 Lab and Podium computers must be joined to the UTRGV Domain under the Lab and Podium Group (OU)

7.2 Hostnames

7.2.1 All Lab and Podium computers hostnames must adhere to the UTRGV Computer Naming Standard

7.3 All Lab and Podium computers must be physically secured

7.4 Screen Lockout

7.4.1 All Lab computers must be configured to auto-lock automatically after a maximum of 30 minutes of inactivity

7.4.2 All Podium computers must be configured to auto-lock and be password protected after a maximum of 60 minutes of inactivity

7.3 Automatic Restart

7.3.1 All Lab and all Podium computers must be configured to restart automatically after a maximum of 180 minutes of inactivity

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

7.4.1 All Lab and Podium computers must be configured to reset to a standard image after a reasonable amount of time when not in use

7.4.2 Systems must be configured such that no user information is permanently saved on system upon system restart or user log-out or in the event of system failure, power outage, or other incidents

7.2 Non-Compliance and Exceptions for Labs and Podiums computers

7.2.1 For individuals with specific software requirements – if any of the requirements contained within this standard cannot be met on applicable information you use or support, the Service Request Process must be followed to address any associated risk

8. Roles and Responsibilities

8.1 **End User:** Ensures that the any computer 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

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

8.3 **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

9. Non-Compliance and Exceptions

9.1 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

9.2 Computers which do not adhere to this standard, lack required security software or otherwise pose a threat to UTRGV information resources may be immediately disconnected by UTRGV from any UTRGV network without notice

9.3 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

10. 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