The University of Texas Rio Grande Valley
Information Security Office

Portable System Check Out 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, 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 computing systems 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, and students
b. On-Campus and Off-Campus Use:
    a. Short-term loan: laptops, MS Surface, iPad
        i. Less than 4 days
    b. Long-term loan: laptops, MS Surface, iPad
        i. More than four or more days but less than one month

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 UTRGV employees, students, consultants, vendors, contractors, and other affiliated persons with a UTRGV sponsored account, who operate a computing device within the defined scope,

4. Authority

UTS 165, UTRGV AUP

5. Definitions

Portable System – 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

Note: Department is responsible to select suitable option based on the department needs and requirements

Preliminary proposal for Windows computers only:

1. UTRGV Windows 10 setup image:
   a. The following preliminary proposal implementation assumes that the following items are achievable:
      1. System is capable of deleting profiles and able to reclaim disk space (e.g., Delprof2)
      2. There is an automated process of removing all software, data, and information on a computer and reinstalling everything (i.e., reimage)
   b. Encryption
   c. Domain System and User Domain Account
   d. Tanium and Nexpose agents must be installed
   e. All requirements from UTRGV Computer Security Standard

2. Preconfigured image:
   a. Capable of returning to a preconfigured state (e.g., Deepfreeze)
      1. System must be configured such that no information is permanently saved on system upon system restart or user log-out
      2. Computer backups are the responsibility of the computer operator or primary user
   b. Encryption
   c. Domain System and User Domain Account
   d. Tanium & Nexpose agents must be installed
   e. All requirements from UTRGV Computer Security Standard

Preliminary proposal for MacOS, iOS, Android devices:

1. UTRGV setup image:
    a. Encryption
    b. Domain System and User Domain Account
    c. Tanium and Nexpose agents must be installed
    d. All requirements from UTRGV Computer Security Standard

2. Preconfigured image:
    a. Capable of returning to a preconfigured state (e.g., Deepfreeze)
        i. System must be configured such that no information is permanently saved on system upon system restart or user log-out
        ii. Computer backups are the responsibility of the computer operator or primary user
    b. Encryption
    c. Domain System and User Domain Account
    d. Tanium and Nexpose agents must be installed

7. Roles and Responsibilities

7.1 **Resource Owner**: Ensures that any portable system 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**: Ensures that all portable systems are configured to support the requirements defined in this standard

7.3 **Information Security Office**: Defines and maintains this standard to a level that can define the necessary configurations and security practices to protect UTRGV information resources and ensures 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 as a portable system 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

10. Revision History

Version	Date	New	Original	Modified By
1.0	07/17/2019	Standard Created	N/A	Francisco Tamez
2.0	01/28/2020	Standard Approved by CISO	1.0	Francisco Tamez