The University of Texas Rio Grande Valley
Information Security Office

Computer Security Standard for non-managed Research Network

1. Purpose

This standard establishes the minimum-security requirements necessary to safeguard all computer devices connected to the non-managed Research Network. Its goal is to ensure a secure computing environment by aligning with current best practices, UTS-165, and other applicable regulations. By adhering to these requirements, the University protects its information resources from unauthorized access, data breaches, and other security threats. These standards are mandatory and supplement all other UTRGV policies, as well as federal and state regulations. In cases where this standard conflicts with other compliance requirements, the most stringent standard will apply to maximize protection of university data.

2. Scope

- Applies to All Devices on the Non-Managed Research Network:

  This includes any computer device that connects to the Non-Managed Research Network, whether the device is owned, leased, or managed by UTRGV.

- Covers All Users and Roles:

  The requirements apply to everyone who uses, manages, or supports these devices—faculty, employees, students, consultants, vendors, and contractors.

- Mandatory Compliance:

  All devices, regardless of ownership, must meet the minimum-security requirements outlined in the standard. The Information Security Office (ISO) has the authority to restrict or deny network access to devices that do not comply.

- Academic and Research Use Only:

  The standard is specifically for non-operational systems used for academic or research purposes.

- Wired Systems Only:

  The requirements apply exclusively to wired systems and do not cover wirelessly connected systems.

3. Audience

All employees, faculty, students, consultants, vendors, contractors, and others who operate a Computer within the defined scope.

4. Authority

UTS 165, UTRGV AUP

5. Definitions

Non-managed Research Network –

Refers to a segment of the university's research infrastructure that allows devices not managed by UTRGV central IT to connect to the university's segmented research network, typically for internet access or specialized research functions.

This network is distinct from the managed network in that:

- Devices are not domain-bound or centrally managed by UTRGV IT.
- Users are responsible for local device management, including compliance with security standards.
- It supports research flexibility, especially for faculty students, who require specialized access for computing equipment.

Computer: Any electronic device capable of processing, storing, or transmitting data. This includes, but is not limited to, desktop workstations, servers, laptops, tablets, and smartphones, whether physical or virtual.

Medical Device Computer: A computer or computing device that is physically connected to a medical device for the sole purpose of controlling, monitoring, or managing the medical device.

Portable Computer: Any computer that is designed for mobility and is battery powered, such as laptops, tablets, and smartphones.

Software Firewall: A software application that monitors and controls incoming and outgoing network traffic based on predetermined security rules, providing protection against unauthorized access and network-based threats.

Endpoint Detection & Response (EDR): A security solution that continuously monitors end-user devices to detect, investigate, and respond to cyber threats and suspicious activities.

Network Vulnerability Agent: A software tool installed on a device to scan for and report security vulnerabilities, helping ensure the device remains protected against known threats.

Disk Encryption: A security technology that converts data stored on a disk into unreadable code, which can only be accessed or decrypted by authorized users with the correct credentials.

Authentication Logs: Records generated by a computer system that document user authentication events, such as logins, logouts, and failed access attempts.

Segregated VLAN: A Virtual Local Area Network (VLAN) that is isolated from other networks to restrict access and enhance security for devices connected to the Research Network.

MAC Address: A unique identifier assigned to a network interface for communications at the data link layer of a network segment.

IP Address: A numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.

NAC (Network Access Control): A security solution that enforces policies for network access, ensuring only authorized and compliant devices can connect to the network.

Local Administrator Account: A privileged account on a computer that has full access to system settings and configurations, typically used for maintenance and support.

Backup: A copy of data stored separately from the original, used to restore information in case of data loss or system failure.

Vendor-Managed Device: A device that is maintained, configured, or supported by an external vendor, rather than by UTRGV IT staff.

Confidential or Sensitive Data: Information classified by UTRGV as requiring protection due to legal, regulatory, or institutional requirements. Refer to the UTRGV Data Classification Standard for specific guidance.

6. Standard Details for all UTRGV and Non-UTRGV devices

6.1 System Requirements for all computers

6.1.1 Host Naming Standard

All computers must adhere to the following standards:

First three characters of the host name:

- RDW – Research Desktop Windows
- RLW – Research Laptop Windows
- RDM – Research Desktop Mac
- RLM – Research Laptop Mac
- RDL – Research Desktop Linux
- RLL – Research Laptop Linux

Next five characters:

- UTRGV Tag Number (unique identifier for the device)

Any additional characters:

- At the discretion of the system owner

Example:

- A Windows research desktop might be named: RDW12345 (where 12345 is the UTRGV Tag Number)

6.1.2 Operating System and Application Updates

6.1.2.1 All computers must have the latest security updates and patches installed for both operating systems and applications. Updates should be applied within a month upon release to minimize exposure to vulnerabilities.

6.1.2.2 Unsupported or end-of-life operating systems and software (i.e., those no longer receiving vendor security updates) are strictly prohibited.

6.1.3 Malware Protection

Approved antivirus or anti-malware software must be installed and actively running on all computers.

Malware definitions and protection engines must be kept up to date through automatic or scheduled updates.

6.1.4 Software Firewall

A software firewall must be enabled to monitor and control network traffic, providing an additional layer of protection against unauthorized access.

6.1.5 Required agent installation

6.1.5.1 Endpoint Detection & Response (EDR)

All computers must have an approved Endpoint Detection & Response (EDR) solution installed and enabled to detect, investigate, and respond to security threats.

6.1.5.2 **Network Vulnerability Agent**

A network vulnerability scanning agent must be installed to continuously assess and report on system vulnerabilities.

6.1.5.3 Network Access Control Agent

A network access control agent must be installed to identify, assess and report system health status.

6.1.6 **Password Protection**

6.1.6.1 All computers must be configured to require strong, complex passwords for user authentication.

6.1.6.2 Passwords must comply with University password standards and be changed regularly.

6.1.7 **Logging**

6.1.7.1 Default logging must be enabled for all applications.

6.1.7.2 At a minimum, operating system security activity and authentication logs must be retained and protected from unauthorized modification or deletion.

6.1.8 **Administrative Privileges**

6.1.8.1 For access to elevated privileges, a separate administrator level account must be created.

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

6.1.8.3 Separate non-administrative accounts must be created for regular user activities.

6.1.8.4 Administrative privileges should only be used for tasks that require elevated access and only for the duration necessary.

6.1.9 **Physical Security**

Devices must be physically secured at all times, preferably in locked rooms or cabinets.

When possible, use cable locks or other physical security mechanisms to prevent theft or unauthorized access.

6.1.10 **Endpoint Registration**

All devices must be registered with IT, including IP address, MAC address, and physical location, for identification and network access control.

6.1.11 **Backup and Recovery**

6.1.11.1 Computer backups are the responsibility of the device operator or primary user.

6.1.11.2 A documented backup standard must be developed, implemented, and followed to ensure data recovery in case of loss or failure.

6.1.12 Disk Encryption

Disk encryption must be enabled on all computers that store or access confidential or sensitive University data.

Encryption keys must be managed securely and access restricted to authorized personnel.

6.1.13 **Network Segmentation**

6.1.13.1 Devices storing or accessing sensitive data must be placed on a segregated VLAN with limited internet access (only ports 80/443).

6.1.13.2 Wireless connectivity must be disabled.

6.2 Access Requirements for all computers

6.2.1 **Application Access Management**

6.2.1.1 Access to applications must be administratively supported by the designated user or owner.

6.2.1.2 Maintain a documented list of all individuals with access to each application.

6.2.1.3 Provisioning and de-provisioning of accounts must be logged, including dates and responsible personnel.

6.2.1.4 Conduct quarterly access audits to verify appropriate access levels and remove unnecessary accounts.

6.2.1.5 Retain audit records for a minimum of three years, or for the duration of the grant or project, whichever is longer.

6.2.2 **Remote Access**

6.2.2.1 Remote access to computers must be done via UTRGV VPN connection with MFA enabled.

6.2.2.2 Access by external vendors or collaborators must be initiated by a local administrator or authorized user and documented.

6.2.3 **Access Review and Monitoring**

6.2.3.1 Regularly review access logs and authentication records to detect unauthorized or suspicious activity.

6.2.3.2 Implement automated alerts for failed login attempts or unusual access patterns.

6.2.4 Compliance

6.2.4.1 Ensure all access controls comply with University policies, federal and state regulations, and grant requirements.

6.2.4.2 Report any unauthorized access or access control failures to the Information Security Office immediately.

6.3 Storage Requirements - Storage requirements applies to all 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 Data Classification

6.3.1.1 All stored data must be classified according to the UTRGV Data Classification Standard.

6.3.1.2 Appropriate safeguards must be applied based on the classification level of the data.

6.3.2 Retention and Disposal

6.3.2.1 Data retention must comply with University policies, grant requirements, and applicable regulations.

6.3.2.2 Secure data disposal procedures must be followed when data is no longer required, including the use of approved data wiping or physical destruction methods.

6.3.3 Access Controls

6.3.3.1 Access to stored data must be restricted to authorized personnel only.

6.3.3.2 Maintain records of data access and modifications where feasible.

6.3.4 Documentation

Maintain documentation of backup procedures, encryption methods, and access controls for audit and compliance purposes.

6.4 Networking requirements for all computers that store or access UTRGV confidential or sensitive data.

6.4.1 Network Segmentation

6.4.1.1 Devices that store or access UTRGV confidential or sensitive data must be placed on a segregated VLAN within the Research Network.

6.4.1.2 Segregated VLANs must restrict internet access to only essential ports (e.g., ports 80 and 443 for web traffic).

6.4.1.3 The VLAN must be configured to prevent default internal connections with the UTRGV operational network.

6.4.2 Wireless Connectivity

Wireless access is not authorized and must be disabled on all devices.

6.4.3 Device Registration

All devices connected to the Research Network must be registered with IT, including IP address, MAC address, physical location, asset owner, and technical contact.

Registration enables identification and enforcement of network access control (NAC) policies.

6.4.4 Network Access Control (NAC)

6.4.4.1 Installation of the NAC agent is required for posturing and compliance verification.

6.4.4.2 Only authorized and compliant devices may connect to the Research Network.

6.4.5 Inventory Management

6.4.5.1 All network-connected equipment must be registered for inventory purposes, including:

- Make and model #
- Asset owner
- Asset owner email
- Technical contact
- Physical location

7. Roles and Responsibilities

7.1.1 Staff and Faculty

7.1.1.1 Ensure that all computers they own or operate comply with the security standard.

7.1.1.2 Complete required security awareness training courses, including password creation, information classification, and privileged user responsibilities.

7.1.1.3 Collaborate with UTRGV IT Computer Support Staff for guidance, configuration, and ongoing compliance.

7.1.1.4 Promptly report security incidents, vulnerabilities, or non-compliance to the Information Security Office.

7.1.2 UTRGV IT Computer Support Staff

7.1.2.1 Computer Support staff will aid to configure, maintain, and support each system to meet the technical requirements as defined in this standard.

7.1.2.2 Provide technical assistance and guidance to staff, faculty, and other users.

7.1.2.3 Conduct periodic audits and reviews to verify compliance and address any gaps.

7.1.2.4 Assist with device registration, network segmentation, and implementation of security controls.

7.1.3 Information Security Office (ISO)

7.1.3.1 Define, maintain, and update this standard to ensure alignment with UT System, state, and federal policies.

7.1.3.2 Monitor compliance, investigate violations, and manage the security exception process.

7.1.3.3 Provide oversight, risk management, and incident response for the Research Network.

7.1.3.4 Communicate changes in standards, policies, or procedures to all stakeholders.

7.1.4 Vendor Support Staff

7.1.4.1 Ensure that vendor-managed devices meet all applicable requirements of this standard.

7.1.4.2 Work with UTRGV IT Computer Support Staff to maintain compliance and address technical issues.

7.1.4.3 Provide documentation and justification when exceptions to standard requirements are necessary.

7.1.4.4 Cooperate with audits and respond to requests for information or remediation.

7.1.5 All Users (including students, consultants, contractors, and external collaborators)

7.1.5.1 Adhere to all security requirements when using, managing, or supporting devices connected to the Research Network.

7.1.5.2 Protect confidential and sensitive data in accordance with University policies and standards.

7.1.5.3 Report any suspected security incidents, unauthorized access, or policy violations to the Information Security Office or IT support staff.

8 Non-Compliance and Exceptions

8.1.1 Immediate Remediation of non-compliance

8.1.1.1 Computers that do not adhere to this standard lack required security software, or otherwise pose a threat to UTRGV information resources may be immediately disconnected from any UTRGV network without notice to protect University assets.

8.1.2 Exception Process

8.1.2.1 If any requirement within this standard cannot be met for applicable information resources, the Security Exception Process must be followed.

8.1.2.2 Exception requests must include documentation and justification, outlining the specific requirement, reason for non-compliance, and proposed risk mitigation measures.

8.1.2.3 All exceptions are subject to review and approval by the Information Security Office (ISO). Please note that submission alone does not guarantee approval.

8.1.3 Reporting and Notification

8.1.3.1 Non-compliance may result in notification of supervisors, department heads, or project managers.

8.1.3.2 All suspected security incidents, unauthorized access, or policy violations must be reported promptly to the Information Security Office or IT support staff.

8.1.4 Disciplinary Action

8.1.4.1 Non-compliance with this standard may be subject to disciplinary action in accordance with applicable UTRGV rules and policies, up to and including loss of network privileges or further administrative action.

8.1.5 Continuous Review

8.1.5.1 The Information Security Office will monitor compliance, investigate violations, and manage the security exception process.

8.1.5.2 Periodic audits will be conducted to verify adherence and address any gaps.

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
1.0	10/7/2023	Initial Draft
2.0	11/20/2025	2nd draft for evaluation
3.0	11/25/2025	Standard approved for posting