THE
UNIVERSITY
OF RHODE ISLAND

Policy on IT Endpoint Protection

Policy Title	**Policy on IT Endpoint Protection**
Policy #	07.102.2
Policy Owner	Chief Information Officer
Contact Information	Questions regarding this policy should be directed to the Chief Information Officer at (401) 874-4599
Approved By	Administrative Policy Committee
Effective Date	June 7, 2022
Next Review Date	No later than June 30, 2027
Who Needs to Know About this Policy	All faculty, staff, students, University Affiliates, vendors, and guests of the University, as well as any other parties granted access to University IT Resources.
Definitions	**Confidential University Data**. All University data that is required to be maintained as private or confidential by applicable law or agreement, or that the University considers and treats as confidential information, whether protectable under law (e.g., trade secrets), or not (other proprietary or sensitive information that the University would not involuntarily disclose except when required by law). **IT Resources**. All computer and telecommunications equipment, software, data, and media, owned or controlled by University or maintained on its behalf. **University Affiliate**. Any individual who is not a faculty member, staff, or student who otherwise has a formal relationship with the University, including but not limited to visiting scholars, visiting students, postdoctoral or other research fellows, professional program participants, adjunct teaching or clinical personnel, volunteers, employees and associates of the URI Foundation and Alumni Engagement, and members of the University of Rhode Island Board of Trustees. Vendors and contractors are not considered affiliates. **University Data**. All data or information held on behalf of the University, created as a result and/or in support of University business, or residing on University IT Resources, including both electronic and paper records. University Data includes personal data (e.g., personal emails to friends, copies of tax returns) of Users that do not relate to University business but that Users voluntarily choose to transmit or store on IT Resources. **User**. Any individual granted access to University IT Resources.

Statutes, Regulations, and Policies Governing or Necessitating This Policy	Family Educational Rights and Privacy Act (FERPA) Gramm-Leach-Bliley Act / Financial Services Modernization Act (GLBA) Health Insurance Portability and Accountability Act (HIPAA) Payment Card Industry Data Security Standard (PCI DSS) RIGL § 11-49.3 (Identity Theft Protection Act of 2015) RIGL s. 5-77.3 (Confidentiality of Health Care Communications and Information Act) University of Rhode Island Policy on Export Control Compliance University of Rhode Island Policy on IT Acceptable Use University of Rhode Island Policy on IT Resources
Reason for Policy/Purpose	To provide rules and guidelines for appropriately securing and managing endpoint protections on University-owned devices and personally-owned devices used for University business.
Forms Related to this Policy	None

Policy Statement

University-owned electronic devices are strategic and vital assets belonging to the University of Rhode Island. As such, these devices must use appropriate security measures and have appropriate security software installed. Personally-owned devices used by the faculty, staff, and Affiliates of the University for conducting University business are subject to the same security provisions. Other groups of Users who access University networks and systems in more limited roles, such as students and guests of the University, must meet minimum standards for security such as installed and active anti-virus / anti-malware protection. In addition, all remote access to University networks or University hosted software or platform must be conducted via the University's VPN service with multifactor authentication (MFA).

Applicability

This policy applies to all Users of University IT Resources including faculty, staff, students, University Affiliates, vendors, and guests. It applies to IT Resources administered centrally as well as those administered by individual colleges or departments; to personally-owned computers and to devices connected to all University networks; and to on-campus computers as well as off-campus computers that connect remotely to the URI network.

User Responsibilities

Users must comply with all sections of this policy and are responsible for the security of all devices and associated data. In addition, Users of any device used to conduct University business, whether that device is University owned or personally owned, must be familiar with and comply with the University's IT Acceptable Use Policy. Users of any electronic device used to conduct University business or to connect to University networks for any purpose may not use these devices for any malicious purpose or illegal activity, including any type of system penetration, software piracy, or activities involving copyright infringement.

Users of all devices are expected to keep the system and all applications fully patched and up to date. The University will provide assistance and automatic patch installation for all University-owned devices (for assistance in meeting this requirement, please contact the ITS Service Desk). Users may not tamper with or uninstall any management or security software installed on the device by the University.

User Privacy

Through device management software, connections to University networks, and use of URI systems, the University could possibly obtain access to a User's technical use information such as location, logs, hardware and software, usage, browser activity, and event history. The University has appropriate physical, electronic, and managerial procedures to restrict access to this technical information. A User's technical information may be used by URI Public Safety, Human Resources, Office of Community Standards, or Student Judicial Conduct to clarify and resolve investigations. Additionally, a User's technical information may be used to diagnose and debug computing equipment, provide individualized assistance to end users, and to support data-informed decision-making processes.

University-Owned Devices

Devices, applications, and accessories provided by the University remain the property of URI and can be revoked or reassigned as needed. All devices must be returned to the University upon separation from the university. The University has full rights to remove unauthorized or modified applications from University-owned devices without notice or warning.

The University allows the use of University-owned devices for the creation and storage of personal data provided the creation and retention of such data does not impede the functions of the device, its applications, connectivity, or management, or contravene local, state, or federal laws. However, University-owned devices may not be used for political purposes, unauthorized personal economic gain, or in any other way that is inconsistent with the values, mission, and ethics of the University of Rhode Island.

When traveling internationally with University-owned devices, all Users are expected to understand and abide by the guidelines on foreign travel, Export Controls, and other applicable policies and regulations. See the University's policy on Export Control Compliance for more information.

University owned devices are subject to the following provisions:

- All University-owned devices must be linked to unique URI-provided digital identities belonging to individual Users that are managed through central identity provisioning services. University-owned devices shall, subject to exceptions noted below, be managed and supported by the professional IT staff and end-users will not have administrative rights to add, modify, or delete the software and configurations of the devices.
- All University-owned devices shall have appropriate patch management, remote configuration, remote monitoring, and anti-malware software installed and continuously operating. For specific device configuration information, please consult with the IT Security office at security@uri.edu.
- All software installed must be either provided and installed by the University or otherwise approved by the University for installation by the User. Users should understand that unmanaged or unapproved installations compromise the operating environment and constitute a security risk, including the intentional or unintentional spreading of viruses, ransomware, or release of sensitive of Confidential University Data. Requests for software security reviews may be directed to the IT Security Services office at security@uri.edu.
- Hard drives shall be encrypted and this encryption shall not be altered or removed for any purpose.
- To the extent possible, and consistent with applicable law and binding University agreements, Confidential University Data may not be stored on a local device. Master data copies shall be stored in University-

provided and approved data storage systems. When local data copies are absolutely necessary, the data shall be erased from the device as soon as possible.

- If a device is used from a remote location, the device shall always use the URI Virtual Private Network (VPN) service with multifactor authentication (MFA) for network access.

Innovation and research are part of the core mission of the University of Rhode Island. The pursuit of new knowledge may often necessitate the design and development of new software, testing of new network protocols, and similar activities. When such uses conflict with these provisions, every attempt should be made to separate and isolate these activities to endpoints on unique parts of the network or unique devices. For assistance with setup and deployment, please contact the IT Security Services Office at security@uri.edu.

Personally-Owned Devices

The University recognizes that many of its community members, including students, employees, affiliates, and guests may access IT Resources through personally-owned devices. However, to ensure security of the University's IT Resources and provide consistency of operations, the use of these devices are controlled by the following guidelines and rules.

All personally-owned devices connecting to University networks or utilizing URI-provided services in cloud environments shall have anti-virus and anti-malware applications installed and active and must be kept up to date with the latest updates, patches, and fixes. The use of any device that is "jailbroken," "rooted," or has been subject to any other method of altering or disabling of built-in protections is not permitted for use in the conduct of any University business. To this end, the University reserves the right to deny access to both University networks and services to systems that are not aligned with current security best practices, such as devices that are no longer being updated by their manufacturers, devices displaying indications of hacking or viruses, and similar devices and configurations.

The University recognizes that many Users use personally-owned smartphone and tablet devices for common-use communication and various productivity applications. When these devices are used for conducting University business they shall have appropriate remote wipe and reset capability. Users are responsible for backing up and restoring personally-owned devices and associated data. Users must provide access to personally-owned devices when notified that the device is needed for e-discovery, litigation hold purposes, NCAA Investigations, and/or any other governmental or legal requirements.

Faculty and staff should avoid the use of personal laptops and desktops for conducting University business, including all administrative tasks, grading of student work, and sponsored research activities. When such use is necessary and involves accessing sensitive or Confidential University Data or interacting with University-owned systems using elevated privilege levels (such as User installation, patching or updating, large-scale data uploads or downloads, and similar) the following additional provisions shall apply:

- University-provided device monitoring, device management, and security software must be installed on the device.
- URI Virtual Private Network (VPN) service with multifactor authentication must be used.
- The device must utilize unique user identities with strong password or biometric identity verification in place.

Policy Enforcement

Disciplinary measures for violations are normally applied by the University office or department appropriate to the violation. Violators may be subject to additional sanctions, penalties, or disciplinary actions imposed by the University and are also subject to international, federal, state, and local laws governing interactions that occur on information technology systems and the Internet.

The University may restrict or deny access to any University IT resource temporarily or permanently to any endpoint device, or its associated user found to be in violation of this policy. Responses to violations may include eliminating access to the networks, blocking external access to the system, or physical seizure of University assets.

Exceptions

Any exceptions to the security provisions of this policy must be approved in writing by the Chief Information Security Officer.

Policy Review and Revisions

(Versions earlier than the first policy number may be paper only)

Policy #	Effective Date	Reason for Change	Changes to Policy
07.102.1	August 31, 2021	n/a	n/a
07.102.2	June 7, 2022	Scheduled Review	Adds requirement for all University-owned devices to meet endpoint protection standards; enforcement language added.