THE
UNIVERSITY
OF RHODE ISLAND

Policy on IT Data, Systems, and Services

Policy Title	**Policy on IT Data, Systems, and Services**
Policy #	07.105.1
Policy Owner	CIO and Associate VP for Information Technology
Contact Information	Questions regarding this policy can be directed to the CIO and Associate VP for Information Technology at (401) 874-4599
Approved By	President of the University of Rhode Island
Effective Date	August 21, 2026
Next Review Date	No later than August 31, 2031
Who Needs to Know About this Policy	All individuals granted access to interact with University IT Resources including, but not limited to, all faculty, staff, students, and University Affiliates.
Definitions	**Access Credentials.** Information or devices used to verify identity and provide access to Information Technology ("IT") Resources, such as usernames, passwords, PINs, digital certificates, and security tokens. **Administrator.** For the purposes of this policy, any individual who administers Systems, servers, and/or services. Additionally, any University staff designated as responsible for Third-Party Services will be considered the Administrator of such services. **Authentication.** The process of verifying the identity of an IT User, process, or device, often as a prerequisite to allowing access to IT Resources. **Authorization.** The process of granting or denying specific access rights or privileges to an IT User, program, or process. **Computer.** For purposes of this policy, any digital electronic computing device. **Data Breach.** An incident in which University Data is accessed, disclosed, or used by an unauthorized individual. **Data Classifications.** Classifications as defined in the *URI Data Classification Schema and Guidelines*. Below are brief definitions for convenience; however, if the definitions change in the *URI Data Classification Schema and Guidelines*, those definitions shall prevail: ● **Public.** Data or information that is publicly available or that, if disclosed, would cause no harm to URI or its community. ● **Internal.** Data or information that URI prefers to keep confidential but that, if disclosed, would cause only minor harm to URI or its community.

	● **Confidential.** Data or information for which unauthorized disclosure would cause significant harm to URI or its community. This classification also includes sensitive business information and certain protected information that is highly valuable to the University. ● **Restricted.** Data or information for which unauthorized disclosure could result in major and possibly irreparable harm to URI or its community. This includes highly sensitive business information and information that is protected by statutory, regulatory, and/or contractual requirements. Restricted information includes information designated as Controlled Unclassified Information (CUI) under federal regulations, FERPA- and HIPAA-protected information, export-controlled data, and any other information requiring security clearance or government-mandated access authorization. **Data Integrity.** The accuracy and consistency of data stored in a database, data warehouse, or other construct. **Endpoint Device.** Any device that connects to the University's network, including but not limited to desktops, laptops, tablets, smartphones, and servers. **Encryption.** The process of converting readable information or data into a form that is readable only by authorized persons or systems. **Firewall.** A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. **Incident Response.** The approach and procedures followed when a security breach or Data Breach or other cyber incident occurs; including detection, investigation, containment, eradication, and recovery. **Chief Information Security Officer ("CISO")**. The individual responsible for overseeing the development, implementation, and maintenance of the organization's information security program. **IT Resources.** All Computer or telecommunications equipment, software, data, and media owned or controlled by the University of Rhode Island or maintained on its behalf. **IT Service.** All Computer software or hardware components that support a multi-user environment maintaining any aspect of URI operations, including teaching, research, service, or administration. **IT User ("User").** Any individual who is granted access to interact with University IT Resources in the course of their work, studies, or affiliation with the University of Rhode Island. **Laws and Regulations.** All applicable international, federal, state, and local laws, statutes, regulations, ordinances, rules, court orders, and other legally binding governmental or regulatory requirements. **Malware.** Software that is specifically designed to disrupt, damage, or gain Unauthorized Access to Computer systems, or conduct a Data Breach.

Multi-Factor Authentication ("MFA"). A security system that requires more than one method of Authentication from independent categories of credentials to verify the User's identity for a login or other transaction.

Patch Management. The process of managing updates for software applications and technologies, including the deployment of patches to fix vulnerabilities and improve functionality.

Personally Identifiable Information ("PII"). Information relating to an identified or identifiable individual, including but not limited to names, identification numbers, location data, online identifiers, or factors specific to physical, physiological, genetic, mental, economic, cultural, or social identity.

Role-Based Access Control ("RBAC"). An approach to restricting system access to authorized Users based on their roles within an organization.

Security Awareness Training. Programs designed to educate Users about cyber threats, security policies, and best practices to protect IT Resources and University Data.

Security Office. The office of the CISO and their staff.

System. Any Computer or telecommunications network or configuration, server, and service that handles or stores University Data or provides an IT Service to the University of Rhode Island.

Third-Party Services. Services, Systems, platforms, or tools provided by external vendors or contractors that are procured and/or otherwise used by the University to support its IT infrastructure and general operations.

Unauthorized Access. Any access, use, entry, or attempt to access, use, or enter any System(s), or elevation of access privileges, by individuals or programs which do not have explicit permission to do so.

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. This term refers to all data or information created as a result of, or in support of, University Operations, as well as all data residing on University IT Resources, including both electronic and paper records. For detailed guidelines and classifications, refer to the *URI Data Classification Schema and Guidelines*. University Data encompasses:

- **University-Owned Data.** Data that is created, stored, transmitted, or processed as part of University Operations, and any information that is expressly required for the administration and functioning of University departments, encompassing all categories of data except where ownership is defined as

	belonging to the individual under a University policy, faculty contract, or other University-executed contracts or agreements. Confidential and Restricted University Data (e.g. FERPA, HIPAA, research, personnel, and other protected or regulated data) are included. For the avoidance of doubt, University-Owned Data does not include faculty intellectual work product in which a faculty member holds rights under the University's Intellectual Property Policy, applicable collective bargaining agreements, or faculty contracts, including (as applicable) research data generated from individual faculty inquiry, unpublished manuscripts, course materials in which the faculty member holds copyright, and creative works. ● **Personal Data.** Data created, transmitted, or stored by a User that does not relate to University Operations. Personal Data that is voluntarily transmitted or stored on University IT Resources by Users is not considered University Data for the purposes of this policy, provided that: a. The use is non-commercial and intermittent, such as checking personal emails, managing personal appointments, or listening to music; and b. The activity does not interfere with the operation of University IT Resources, complies with all relevant University policies regarding acceptable use, and adheres to all Laws and Regulations. **University Network.** Any wired or wireless network, on-campus or remote, that is owned, operated, managed, or licensed by the University of Rhode Island, including University-managed remote access and cloud-based networking services. **University Operations.** All teaching, research, community engagement, and business functions, as well as any other official activity of the University. **Virtual Private Network ("VPN").** A technology that creates a safe and encrypted connection over a less secure network, such as the internet. **Virtualization.** The creation of a virtual (rather than actual) version of something, such as a virtual Computer hardware platform, operating system, storage device, or network resources. **Vulnerability.** One or more weaknesses in an IT system that can be exploited by threats to gain Unauthorized Access to information or disrupt critical processes.
Statutes, Regulations, and Policies Governing or Necessitating This Policy	Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801–6809 (Financial Privacy). Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, and implementing regulations at 34 C.F.R. Part 99. Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. § 3551 et seq. Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. §§ 1320d–1320d-9 (Standards for Privacy of Individually Identifiable Health Information), and implementing regulations at 45 C.F.R. Parts 160 and 164.

	R.I.G.L. §§ 11-49.3-1 to -7 (Identity Theft Protection Act of 2015). R.I.G.L. §§ 36-14-1 to -21 (Rhode Island Code of Ethics). R.I.G.L. §§ 38-2-1 to -16 (Rhode Island Access to Public Records Act). R.I.G.L. §§ 5-37.3-1 to -12 et seq. (Rhode Island Confidentiality of Health Care Communications and Information Act). Payment Card Industry Data Security Standard (PCI DSS). *Policy on Approval and Execution of Contracts and Other Binding Documents.* *Policy on Conflict of Interest and Commitment* *Policy on HIPAA Privacy and Security.* *Policy on Intellectual Property.* *Policy on the Rights of Students Pursuant to FERPA.*
Reason for Policy / Purpose	The purposes of this policy are to 1) establish standards for the acceptable use of IT Resources; 2) ensure the protection and security of IT Resources, University Data and IT Users; 3) require appropriate protections on all Endpoint Devices used for University Operations; 4) define the responsibilities of Administrators to protect and secure IT Resources and University Data; and 5) comply with Laws and Regulations.
Forms Related to this Policy	None

Policy Statement

The University of Rhode Island ("University" or "URI") is committed to ensuring the protection and integrity of its digital infrastructure, data and information, the security of all community members, and compliance with Laws and Regulations. Concurrently, the University is committed to its mission and foundational values, including academic freedom, the freedom to learn, teach, create, and conduct research, and the right to privacy; and recognizes that these are essential to fostering an environment of intellectual exploration, innovation, and rigorous scholarship. The University seeks to safeguard its IT Resources in ways that are consistent with and respectful of these commitments.

All IT Users ("Users") must comply at all times with 1) Laws and Regulations; 2) University policies (including this policy) and ethical codes; 3) contractual obligations; and 4) accepted industry standards for information security and responsible use.

This comprehensive IT policy encompasses most aspects of URI's Information Technology, computing, and related services. The policy addresses acceptable use, endpoint protection requirements, service protection, email retention, access to University systems, data protection, and personal responsibilities. This policy supersedes several prior University IT-related policies (as enumerated at the end of the document). However, nothing in this policy shall be deemed to supersede, contradict, or override any provisions contained in collective bargaining agreements, other contracts between the University and any third parties, Laws and Regulations, or any other University Board of Trustees policy that may conflict with this policy. In the event of any such conflict, the terms of

the collective bargaining agreements, contracts, Laws and Regulations, or URI Board of Trustees policy shall prevail.

This policy applies to all individuals who are granted access to interact with University IT Resources, including, but not limited to all faculty, staff, students, and University Affiliates. The comprehensive nature of this policy ensures that all parties are governed by consistent standards and practices, fostering a secure and respectful digital environment that aligns with the University's commitment to academic excellence and integrity.

I. Responsible and Acceptable Use

All Users must utilize University IT Resources in a manner that supports the University's mission and foundational values, protects the integrity and security of URI's digital infrastructure, and respects the rights and privacy of community members. This section outlines expectations and guidelines for ethical and appropriate use of University IT Resources, and establishes standards for responsible and acceptable use to maintain a secure and productive IT environment conducive to academic freedom and innovation.

A. Responsible and Appropriate Use: Users are expected to:

1. Use University IT Resources for conducting University Operations;
2. Respect the privacy interests of other Users and adhere to University policy and access and monitoring practices; and
3. Avoid interfering with the activities of others or using a disproportionate share of IT Resources.

B. Prohibited Activities: Users may not use University IT Resources to:

1. Deprive access to individuals otherwise entitled to access University information.
2. Engage in activities that violate any Laws and Regulations, applicable University policies, or materially interfere with University Operations. This prohibition shall not be construed to restrict bona fide research, scholarly inquiry, teaching, or creative work conducted in alignment with Laws and Regulations, applicable University policies, research ethics, and human subject protections.
3. Send unsolicited messages to a large number of recipients ("spamming"). This prohibition is not intended to restrict authorized communications to established University distribution lists, official University announcements, or other communications conducted in the course of University Operations.
4. Consume an unauthorized disproportionate share of networking resources (e.g., misuse of peer-to-peer applications), or otherwise make excessive use of IT Resources.
5. Deliberately cause any denial of service, including flooding, ICMP attacks, or the unauthorized automated use of a service intended solely for human interaction.
6. Interfere with the proper functioning of the University's IT Resources or unreasonably interfere with the ability of others to make use of those resources.
7. Use IT Resources in a manner that impinges upon the rights of any person protected under the United States or Rhode Island Constitutions; any Laws and Regulations; or any University policy.
8. Access protected resources without Authorization, including another User's account, private data, or non-public Systems or hosts; or enable or facilitate such unauthorized access by others.
9. Circumvent, tamper with, remove, disable, alter, bypass, or interfere with University-required security, monitoring, logging, management, access-control, Encryption, or compliance controls on University IT Resources or University-owned Endpoint Devices, except as expressly authorized under approved University procedures, an approved exception, or a documented research or instructional Authorization.
10. Violate copyright laws in connection with their University activities. Copyright violations include reproducing, distributing, or broadcasting copyrighted materials on University IT Resources unless such use is covered by federal fair use guidelines, other copyright law exemptions, or explicit permission

from the copyright owner. Additionally, Users must comply with all license terms and conditions governing the use of University library subscriptions and other electronic resources made available by the University. Unauthorized use may violate copyright or other intellectual property laws and may result in loss of access or other disciplinary action. This information is provided for general guidance and must not be construed as legal advice. In cases of uncertainty or specific questions about copyright law and its application in the context of University activities, Users may consult the Office of the General Counsel (OGC).

11. Engage in any other activities specifically prohibited by this policy and any other applicable University policies.

C. Training Requirements: All Users, including faculty, staff, students, and University Affiliates, must successfully complete annual Security Awareness Training. Additionally, those who manage Restricted Data must also take and pass annual domain- and regulatory-specific training, such as FERPA, HIPAA, Payment Card Industry (PCI), or other relevant and required training. Users authorized to perform administrative functions, whether or not designated as Administrators, must also successfully complete annual training in threat detection, mitigation, and recovery strategies as appropriate for the systems they manage.

D. Storage of University Records and Operational Documents: In accordance with the *Policy on Records Management*, University records and operationally essential documents must be stored in University-approved repositories that are institutionally owned or governed by a department, role, program, or shared University function, and not solely in a location tied to a single individual User account or personal Endpoint Device.

This includes, but is not limited to, administrative and operational documents, financial records, student or employee records, research-related records subject to institutional oversight, compliance materials, legal or audit-related materials, and communications or documentation that support official decisions or University business activities.

Individual User storage locations are not appropriate systems of record for such materials, even when those locations are provided by the University or shared with other Users. This includes, but is not limited to, folders or files stored in an individual User's University-provided Google Drive, OneDrive, Box, email account, or similar service that is tied to a single person rather than a department, role, program, or shared function. Where IRB protocols, data-use agreements, sponsor requirements, University policies, or other legal obligations specify particular data-handling arrangements that impose requirements in addition to or more stringent than those set forth in this section, those requirements govern. Data-use agreements shall be reviewed and approved through the University's contract review processes and shall not authorize data-handling arrangements that would otherwise violate this policy without an approved exception. Nothing in this section alters rights established under the University's Intellectual Property Policy or applicable faculty contracts.

Users may temporarily create, access, or store working copies in individual accounts or on Endpoint Devices as permitted by this policy and applicable procedures, provided that such locations are not relied upon as the sole authoritative copy or system of record. Materials stored solely in an individual User's account or on an individual Endpoint Device may become inaccessible or be deleted when that User changes roles, separates from the University, or when the account or device is deactivated, reassigned, or retired.

The University's *Policy on Records Management* governs the retention, management, disposition, preservation, and production of University records and must be followed.

E. Confidentiality, Security, and Handling of University Data: Users must access University Data solely for conducting University Operations and only as permitted by Laws and Regulations, contracts, and policies. This ensures the integrity and security of University Data and URI's digital infrastructure while upholding the University's commitment to privacy rights and academic freedom. Unauthorized attempts to access data on Systems are strictly prohibited. Users must maintain all records containing University Data in accordance with the applicable records retention requirements, Laws and Regulations**,** contractual requirements, and University policies to comply with legal obligations and support institutional accountability.

Users are prohibited from using any unapproved Third-Party Services (including artificial intelligence (AI) technologies), no matter how access is obtained, to create, store, transmit, process, or handle Confidential and/or Restricted University Data. This prohibition applies to student records protected under FERPA, protected health information (under HIPAA or applicable state law), Confidential or Restricted research data, personnel records, and other protected or regulated data as identified in the Data Classifications. Examples of prohibited uses include, but are not limited to, entering such data into unapproved AI assistants, auto-graders, collaboration platforms, spreadsheet and database services, or writing tools. Users must submit such services for review and approval through the University's information security, privacy, procurement, and contract review processes before any use with protected or regulated data. University-provided and University-managed services (e.g., University email, learning management systems, and other institutionally supported platforms) are considered approved for use in accordance with their intended purpose and applicable data-handling requirements.

The IT Security Office shall maintain a defined pathway for review of research tool requests, with target action windows for standard and expedited review specified in the accompanying procedures. Expedited review is available when a specific time-sensitive basis exists, such as a grant deadline, conference submission, or sponsor milestone, and cannot be used to compensate for an untimely submission. Review timelines may vary with the complexity and risk profile of the request. Requests involving Controlled Unclassified Information, protected health information, or comparably protected or regulated data will be reviewed in accordance with applicable regulatory and contractual obligations, which may extend beyond the standard or expedited target windows. Expedited review reflects prioritization of the review sequence, not a reduction in the substantive risk assessment applied to any request.

1. **Handling of Confidential or Restricted Data:** Any University Data classified as Confidential or Restricted must not be accessed, used, or disclosed without prior Authorization from a designated University official with documented authority to grant such access and an articulated institutional need. This protects the privacy and security of sensitive information. When sharing Confidential or Restricted University Data, Users must ensure that recipients are authorized to receive such information. Confidential and Restricted University Data must not be shared with friends, family members, or any other unauthorized individuals. Additionally, Users must comply with any University-executed vendor contracts or agreements as well as University procurement policies and procedures protecting vendor information (such as software code and proprietary methodologies), to honor contractual obligations and maintain trust.
2. **Requests for Access to Confidential or Restricted Data:** Offices that may handle requests for Confidential or Restricted University Data must follow written guidelines or procedures for authenticating, reviewing, acknowledging, and recording these requests. This ensures transparency, accountability, and compliance with legal and institutional standards. Non-routine requests for Confidential or Restricted University Data must be authenticated and approved by the Office of General Counsel (OGC) and the Director of Records Management. All such requests must be documented,

tracked, and maintained according to the appropriate policy and retention schedule, with an official recorded approval method, to ensure a clear audit trail and accountability.

3. **Data Storage and Encryption:** Confidential and Restricted University Data must be stored on centrally managed or contracted IT Resources as the authoritative system of record. Unless prohibited by Laws and Regulations or binding agreement, such data may be accessed and temporarily stored on Endpoint Devices solely for active use, provided that the device meets University-defined security requirements and that the data is not maintained solely on the device but remains stored in an approved institutional repository. This centralization enhances data security and ensures compliance with this and other institutional policies. Additionally, Confidential and Restricted University Data must be encrypted during transmission over a network and while stored to protect against Unauthorized Access and Data Breaches. Unauthorized Access or disclosure or suspicion of Unauthorized Access or disclosure of Confidential or Restricted University Data must be reported to the Security Office at security@uri.edu within two hours of becoming aware of the incident (or suspected incident) to enable prompt response and mitigation.

F. Access Control and Credential Management: The uniqueness, protection, and non-sharing of Access Credentials are fundamental to maintaining trust, integrity, accountability, and the University's ability to protect privacy, academic freedom, and security. It is imperative that all Users adhere to these principles to ensure the effective governance and security of University IT Resources.

1. **Uniqueness, Protection, and Non-Sharing of Access Credentials:** While using University IT Resources, Access Credentials must be maintained securely and must be unique and distinct from any Access Credentials used to access non-University Resources. These credentials must not be shared or disclosed to anyone. Each User will be held responsible for all activities conducted using their Access Credentials, absent evidence that the credentials were compromised through no fault of the User and that the User promptly reported the compromise.

   No individual may use another person’s Access Credentials to access University IT Resources. Credential sharing is prohibited.

   Exceptions may be granted only under extraordinary circumstances where no reasonable technical alternative exists, such as time-critical emergency response or system recovery. Any such exception must be explicitly approved in writing by the Chief Information Security Officer (CISO) or their designee, must be documented, time-limited, and scoped to the minimum access necessary, and must follow the procedures outlined in the procedures accompanying this policy. Upon expiration or completion of the approved activity, all shared credentials must be revoked and replaced in accordance with University security standards.

   Sharing Access Credentials is strictly prohibited outside these exceptional circumstances due to the severity of the risks involved. Sharing credentials obfuscates accountability, reduces the utility of logs and audit trails, and significantly increases the risk of violating Laws and Regulations, and University policies. Both the owner of the Access Credentials and the individual granted or otherwise obtaining access can be held responsible for violations of this policy or failure to follow related procedures.

2. **Multi-Factor Authentication and Remote Access Security:** All electronic devices, including personal computers, phones, or other devices used to access, create, transact, or store University IT Data or IT Resources, including email and text messaging, must be password protected in accordance with University requirements. Passwords must be changed whenever there is suspicion that the password has been compromised. All University-issued mobile computing devices must be encrypted.

All remote access to University IT Resources must be accomplished using the approved University Multi-Factor Authentication (MFA) methods.

Any unattended portable Computers, phones, and other computing devices must be physically secured.

3. **Personal Device Use and Records Obligations:** If University Data is created or stored on a User's personal Computer, phone or other Endpoint Device, or in databases that are not part of the University's IT Resources, this data and these devices are subject to the University's *Policy on Records Management*; remain subject to applicable Laws and Regulations, including the Rhode Island Access to Public Records Act, subpoenas, court orders, audits, investigations, litigation discovery, and other requirements applicable to University IT Resources; and must be made available to the University upon request. See Section III.D. for additional requirements applicable to personally owned Endpoint Devices used for University Operations.

G. Personal Use of IT Resources: The University recognizes the importance of allowing reasonable, light personal use of IT Resources (such as University-provided email accounts) that does not interfere with University Operations or violate University policies. Users are expected to conduct any such personal use responsibly and in a manner consistent with the University's mission and foundational values, recognizing that use of IT Resources reflects on both the User and the University. This balance supports a positive work and educational environment while ensuring that IT Resources remain available for their primary purposes.

1. **University Employees and Affiliates:** The University provides IT Resources and associated services primarily for business use. However, reasonable personal use by employees and University Affiliates is permitted under the following conditions:
    - The use is not excessive;
    - It does not interfere with normal business activities; and
    - It complies with all University policies and Laws and Regulations.

    Prohibited personal use includes, but is not limited to political campaigning, solicitation, unauthorized financial gain, or conducting business that has no official relationship with the University. Political activity, solicitation, and related conduct by University employees are further governed by the University's *Policy on Conflict of Interest and Commitment* and the Rhode Island Code of Ethics (R.I.G.L. § 36-14).

    Supervisors, appropriate offices, applicable University policies, or Laws and Regulations may impose additional limits on personal use.

2. **Students:** Student personal use of IT Resources must adhere to the provisions of this policy and the University of Rhode Island Student Handbook. Students are expected to use IT Resources responsibly and in a manner that supports their educational activities.

H. Disclosure: The University may share results of investigative actions related to the use of IT Resources with authorized University personnel, outside legal counsel, or law enforcement agencies only at the direction of, or with the approval of, the Office of the General Counsel (OGC). Records created with and/or maintained on University IT Resources may be subject to disclosure under applicable Laws and Regulations, including the Rhode Island Access to Public Records Act, subpoenas, court orders, audits, investigations, and litigation discovery. Any access to User content in connection with disclosure or investigation must comply with the User Privacy section of this policy.

I. Account Eligibility, Offboarding, and Termination of Access: University accounts, Access Credentials, and access to nonpublic University IT Resources may be issued or maintained only for individuals who

have both: 1) an active, documented, formal relationship with the University; and 2) a legitimate institutional need for the specific access granted.

A formal relationship includes current student status, current University employment or appointment, current formal University Affiliate status as defined in applicable University policy or a current University-approved contract or agreement. Absent such a formal relationship, an individual must not be issued University accounts, Access Credentials, or access to nonpublic University IT Resources, and must not be permitted to retain them.

Access must be limited to the minimum necessary for the individual's documented University relationship and institutional need. Access must be modified, restricted, or terminated when the individual separates from the University, changes roles, no longer has a documented institutional need for the access, or no longer has an active formal relationship with the University.

Continued access after separation is not permitted unless described in applicable offboarding procedures.

Standard access changes shall originate from the University's designated authoritative systems of record and be implemented through approved University procedures and automated processes where available. Human Resources, the Office of General Counsel, the Security Office, or other offices authorized by approved University procedures may request expedited restriction or termination of access in sensitive, emergency, involuntary-separation, investigation, compromised-account, or other extraordinary circumstances.

Standard access retention and deprovisioning timelines shall be established in University procedures approved by the appropriate business owners, including Human Resources, ITS, the Security Office, and the Office of General Counsel as applicable. Such procedures must be consistent with the requirement that access may be maintained only while the individual has an active, documented, formal University relationship and a legitimate institutional need for the access.

J. Records and Data Handling: Emails, attachments, files, messages, and other materials that document University Operations may constitute University records and must be preserved, transferred, retained, or disposed of based on their content and applicable records-management requirements, not based solely on the system, format, account, or device in which they reside.

Before a planned separation or role change, Users and supervisors must take reasonable steps to transfer University records and operationally essential documents to appropriate institutional repositories. In the event of a sudden, involuntary, or otherwise unplanned departure, the supervisor or responsible department must promptly follow University procedures to preserve and recover University records, including by contacting Human Resources, Records Management, the Office of General Counsel, ITS, or the Security Office as appropriate.

K. Device Return, Preservation, and Sanitization: All University-owned Endpoint Devices and related equipment must be returned in accordance with University procedures upon separation, role change, request by the University, or when the device is replaced, reassigned, or no longer needed for the User's University role. Users must return University-owned Endpoint Devices in substantially the same configuration and condition in which they were provided, ordinary wear and authorized changes excepted.

Users must not wipe, reset, reimage, destroy, conceal, alter, delete University Data from, remove University-required software from, disable controls on, or otherwise modify a University-owned Endpoint Device before return, except as expressly authorized by University procedures, the Security Office, ITS, the Office of General Counsel, or another authorized University office. This prohibition includes removing,

disabling, altering, or interfering with University-installed or University-required software, operating systems, security tools, management tools, monitoring tools, logging capabilities, Encryption, access controls, or device-management enrollment.

Before a returned device is wiped, reassigned, disposed of, or otherwise made unavailable, University records, legal holds, investigations, public records obligations, audit needs, and business-continuity needs must be preserved in accordance with University procedures, except where immediate security action is required. Personal Data on returned University-owned devices will be handled in accordance with applicable law, University policy, and approved procedures protecting individual privacy to the extent consistent with University obligations.

II. IT Systems Administration, Management, and Security

The purpose of this section is to establish clear rules and guidelines for securing and protecting University Data and Systems, including Endpoint Devices. These guidelines aim to minimize risks to the University while ensuring the protection of academic freedom and reducing challenges for the community. This section applies to all Systems, servers, and services that handle University Data or provide a software/IT Service to the University. It includes Administrators and any staff designated as responsible for Third-Party Services.

A. System Inventory and Status Management: Administrators must maintain a current inventory of all Systems for which they are responsible. For each System, documentation must include the System's name and purpose, physical location, installed software, the nature and sensitivity of University Data handled or stored, and the volume of University Data. In addition, Administrators must

1. **Review and Update:** Regularly review, document, and update the status of these Systems at intervals commensurate with the sensitivity of the data and the criticality of the System, but not less than once per year.
2. **Maintain Documentation:** Ensure that all documentation is comprehensive, up-to-date, and easily accessible for audits and reviews.
3. **Adhere to Best Practices:** Follow industry best practices for inventory management and documentation.

B. Third-Party Systems and Compliance: When Systems are controlled by third parties, Administrators must obtain and maintain positive affirmation from the third party that they meet the required security standards. This can be documented through tools such as the Higher Education Cloud Vendor Assessment Tool (HECVAT) completed by the vendor at the time of purchase. Administrators must also:

1. **Maintain Records:** Keep detailed records of the nature and volume of University Data stored on third-party Systems. Contract owners must ensure that third-party agreements do not interfere with University ownership or assign rights of ownership to University Data that have not been explicitly approved by the Office of the General Counsel (OGC) and the Director of Records Management.
2. **Conduct Regular Assessments:** Conduct regular assessments and reviews of third-party compliance with security standards.
3. **Adhere to Best Practices:** Ensure third parties adhere to industry best practices for data security and system protection.
4. **Document SOPs:** Maintain documented standard operating procedures for managing third-party relationships and ensuring compliance.

C. Data Security and System Protection: Administrators must implement measures to prevent the loss, theft, or ransoming of University Data and disruptions to University functions and servers. These measures

may include full log capture, System intrusion detection, System hardening, and other security protocols as defined by IT Security. Administrators must adhere to industry best practices, which include

1. **Full Log Capture:** Implement full log capture for all systems to ensure complete records of activities and potential incidents.
2. **System Intrusion Detection and Prevention:** Use System intrusion detection and prevention systems to monitor and protect against Unauthorized Access.
3. **System Hardening:** Apply system hardening measures, such as disabling unnecessary services and applying security patches, to reduce vulnerabilities.
4. **Encryption:** Ensure all nonpublic-facing University Data is encrypted at rest and in transit to prevent Unauthorized Access.
5. **Regular Backups:** Perform regular backups of University Data at an appropriate frequency based on the nature of the data. Backups must be encrypted, physically distant from the primary copy, protected against ransomware, and accessible only via Multi-Factor Authentication (MFA).
6. **Disaster Recovery:** Ensure systems are backed up or made recoverable in case of destruction or inoperability. This can be achieved through full-disk snapshots, virtual machine imaging, scripted server recreation, or participation in disaster recovery services.
7. **Patch Management:** Ensure all systems are regularly updated with the latest security patches.
8. **Regular Audits and Monitoring:** Conduct regular security audits and continuous monitoring to detect and respond to security incidents.
9. **Incident Response:** Develop and maintain an Incident Response plan to address security or Data Breaches promptly.
10. **Documentation and SOPs:** Maintain detailed documentation and standard operating procedures to ensure consistent and secure system operations.
11. **User Training and Awareness:** Conduct regular training sessions for users to recognize and respond to security threats.

Administrators must maintain documented standard operating procedures and regularly review and update them to ensure and enforce data and system security.

D. System Network Security: Network access to Systems must be secured to ensure that only authorized network locations and entities can access the Systems. Measures such as Firewalls, intrusion detection/prevention systems (IDS/IPS), and access control lists must be used to enforce this security. Administrators must adhere to industry best practices, which include

1. **Access Control:** Define and enforce who is authorized to access the network.
2. **Firewalls and IDS/IPS:** Utilize Firewalls and IDS/IPS to monitor and control network traffic.
3. **Network Segmentation:** Implement network segmentation to limit access to Restricted Data or Confidential Data and related systems.
4. **Encryption:** Require Encryption for data in transit and at rest.
5. **Regular Audits and Monitoring:** Conduct regular security audits and continuous monitoring to detect and respond to security incidents.
6. **Patch Management:** Ensure that all network devices are regularly updated with the latest security patches.
7. **Incident Response:** Develop and maintain an Incident Response plan to address security or Data Breaches promptly.
8. **Documentation and SOPs:** Maintain detailed documentation and standard operating procedures to ensure consistent and secure network operations.

9. **User Training and Awareness:** Conduct regular training sessions for users to recognize and respond to security threats.

Administrators must maintain documented standard operating procedures and regularly review and update them to ensure and enforce network security.

E. System Physical Security: Systems that are on-premise or under the University's direct physical control must be housed in secure, locked rooms any time the Systems are not under the immediate physical control of the User. Physical access to these rooms must be

1. Controlled using physical keys, electronic locks, or other access control devices.
2. Logged using a logbook or electronic records to track access events.
3. Monitored with video surveillance to ensure ongoing security.

All Users with access must ensure that no unauthorized individuals are permitted to gain entry. Individuals who are not normally authorized and do not customarily have access shall not be left unattended in these secure environments.

All Systems must be locked so as to require Authentication when not in use or not under the immediate physical control of an authorized User in accordance with the IT Security Office's procedures.

Administrators must adhere to industry best practices for physical security and maintain documented standard operating procedures to ensure and enforce these measures.

F. Privileged Access to Systems: Privileged access to Systems must be restricted to the smallest practical number of individuals, with a minimum of two (2) for redundant staff coverage. Privileged access shall be limited to the necessary functions and permissions required for the user's role. All privileged access must employ Multi-Factor Authentication where supported. Systems that do not support MFA must obtain special University approval for use and implement other security measures to mitigate the lack of MFA.

For actions requiring elevated privileges that could significantly impact the University's infrastructure, such as deleting critical accounts or altering core configurations, dual authorization (two-person integrity) must be implemented. This means such actions can only be executed with the approval and presence of at least two authorized individuals.

Systems that implement privilege elevation mechanisms (e.g., sudo) on individual Endpoint Devices may satisfy this requirement without separate privileged accounts, provided that such systems are used by a single user, do not store or process Restricted University Data, do not provide administrative access to sensitive University systems or infrastructure, and maintain logging and attribution for actions taken with elevated privileges.

All actions executed with elevated privileges must be logged in a tamper-resistant log format that includes sufficient detail to identify who performed the action, when it was performed, what was done, and, if possible, why it was done and what was viewed. Logs must employ mechanisms, such as blockchain validation, to ensure that any tampering is detectable.

Privileged accounts must not be used for non-privileged activities. Users must have separate accounts for normal user-level activities and privileged administrative actions. Administrative actions must require either an elevated privilege account that is tied to a single individual and not shared, or must require privilege elevation that triggers logging from the moment of requesting elevated privileges.

Administrators must:

1. Revoke privileged access promptly when an individual no longer requires it.

2. Periodically review all privileged access accounts and remove any that are no longer used. The frequency of these reviews must be appropriate to the sensitivity of the System and University Data, but not less than once per year.

Administrators must adhere to industry best practices for privileged access management and maintain documented standard operating procedures to ensure and enforce these measures.

G. Monitoring and Security Software for Systems: Systems must have University-approved anti-virus, security, and monitoring software installed to protect University Data and Systems. All Systems must have comprehensive logging enabled for all security-related events. Logs must be maintained in a tamper-resistant format and reviewed regularly to detect and respond to potential security incidents.

Administrators must

1. **Install Approved Software:** Ensure all Systems have the necessary University-approved anti-virus, security, and monitoring software installed.
2. **Enable Comprehensive Logging:** Ensure all Systems have full logging enabled for all security-related events, capturing sufficient detail to track activities and identify potential incidents.
3. **Review Logs Regularly:** Regularly review logs to detect and respond to security incidents promptly.
4. **Maintain Tamper-Resistant Logs:** Maintain logs in a tamper-resistant format to ensure their integrity and reliability.

Administrators must adhere to industry best practices for monitoring and security software and maintain documented standard operating procedures to implement and enforce these measures.

Systems that cannot implement University-required anti-virus, security, or monitoring software because those controls would materially interfere with legitimate research or instructional requirements must have a documented exception approved in accordance with the Exceptions section of this policy, must operate within an approved restricted network environment or secure enclave, must not store or process Confidential or Restricted University Data, and may store or process Internal University Data only when justified in the documented exception.

H. Use of Commercial Cloud Services: Non-enterprise End User License Agreements (“EULAs”) and similar agreements (e.g., “click-through” or “clickwrap” agreements) (collectively referred to as "Digital Agreements") that Users agree to when accepting the terms and conditions of services online (e.g., by clicking "I agree" or checking a box or continuing to access or use the services) are legally binding contracts. These agreements fall under the University’s Policy on Approval and Execution of Contracts and Other Binding Documents, which expressly prohibits most Users from individually entering into such agreements. It is the sole responsibility of the User to ensure full compliance with the University’s Policy on Approval and Execution of Contracts and Other Binding Documents and any other applicable University policies and procedures (e.g., procurement requirements) before agreeing to any terms and conditions.

Every IT User is responsible for understanding the contents and terms of each Digital Agreement. These agreements often grant vendors ownership of data and metadata, and/or the right to use, share, sell, and license this information. Such rights can include unlimited, irrevocable permissions, which may pose significant risks to the University, its community, and IT Users themselves. For example, storing sensitive research data or student information on a non-approved platform could lead to Unauthorized Access, Data Breaches, or legal liability. Additionally, Digital Agreements may transfer legal liability to the Users or the University, or significantly limit the legal rights of either.

This section addresses Digital Agreements that would bind the University to new terms, new services, new data-handling arrangements, or new financial or legal obligations. Routine acceptance of terms incidental to the ordinary use of services the University has already reviewed and approved — including re-acceptance of terms upon software launch, session authentication, form submission, or comparable interactions within an approved service — is not within the scope of this prohibition, provided the terms being accepted are the same terms under which the service was reviewed and approved.

The University supports the responsible adoption of emerging technologies while managing risk. Users must use University-administered or University enterprise-licensed services when available. If none exist, Users may use University-approved services (see the Approved Services List maintained by the IT Security Office). If no approved service is available, Users may request to use an alternative service subject to prior written approval from the IT Security Office.

III. Endpoint Protection

The purpose of this section is to establish rules and guidelines for securing and managing endpoint protections on University-owned Endpoint Devices and personally owned Endpoint Devices used for University Operations, minimizing risks to the University while protecting academic freedom and reducing challenges for the community.

A. Applicability: This section applies to all Users of University IT Resources, including faculty, staff, students, University Affiliates, vendors, contractors, and guests. It covers IT Resources administered centrally, by individual colleges or departments, and includes personally owned Endpoint Devices connected to all University Networks, both on-campus and remotely.

B. User Responsibilities: All Users must comply with all sections of this policy and are responsible for the security of all devices and associated data. Any device used for University Operations, whether University-owned or personally owned, must not be used for unauthorized, prohibited, or illegal activities.

All devices used for University Operations must be kept fully patched and up to date in accordance with University requirements. The University may assist with or require automatic patch installation, configuration management, and security updates for University-owned Endpoint Devices.

All Computers connecting to the University's network must run security software prescribed by the Chief Information Security Officer (CISO) to properly secure University IT Resources. This includes, but is not limited to, antivirus software, anti-malware tools, Firewalls, and intrusion detection systems.

Users must ensure that all security patches for operating systems and any used software are applied within five business days of becoming aware of those patches. This proactive approach minimizes vulnerabilities and maintains system integrity. They must also ensure that systems are configured to check for and notify users of available patches automatically to ensure timely updates and protection.

Users must not remove, disable, alter, bypass, interfere with, or attempt to circumvent any University-installed, University-required, or University-approved software, configuration, operating system, management tool, security control, monitoring capability, logging mechanism, Encryption setting, access control, endpoint detection and response tool, anti-malware tool, Firewall, mobile device management profile, certificate, or other technical control on any University-owned Endpoint Device, except as expressly authorized in writing under approved University procedures, an approved exception, or a documented research or instructional Authorization described below.

Users must not root, jailbreak, reimage, replace, downgrade, or materially alter the operating system, firmware, boot configuration, security configuration, device enrollment status, management status, or required software baseline of a University-owned Endpoint Device without prior written Authorization. Use of administrative privileges, technical tools, alternate operating systems, external boot media, virtual machines, or other methods to evade University security, management, logging, monitoring, or compliance controls is prohibited.

Grant-funded, research, instructional, testing, accessibility, repair, or specialized devices may be rooted, jailbroken, reimaged, rebuilt, or otherwise modified only within a documented Authorization. The Authorization may apply to a specific device, class of devices, project, lab, or procedure, but must be documented before the device is modified or before the device accesses University Networks or nonpublic University Data, whichever comes first. The Authorization must identify the responsible User or unit, the device or class of devices, the permitted modifications, the University purpose, permitted Data Classifications, network restrictions, compensating controls, and any review or expiration date. A general research purpose, grant purchase, faculty status, local administrator access, or after-the-fact explanation is not Authorization. Modified devices must not be used to evade University security, management, logging, monitoring, compliance, or records obligations.

The IT Security Office shall maintain a defined intake process for device modification Authorization requests, with a target action window for complete requests specified in the accompanying procedures. The IT Security Office shall also maintain a published list of pre-vetted modification categories (such as approved Linux distributions and approved VPN configurations commonly used in research and instruction) for which standing authorizations are available at the laboratory, research group, project, or course level. Modifications falling within a pre-vetted category may proceed under the applicable standing Authorization; modifications outside the pre-vetted categories require individual authorization prior to implementation. Written Authorization must precede the modification in all cases. Devices that cannot operate within the University's compliance boundary for Controlled Unclassified Information or comparably regulated data shall be configured to remain outside that boundary — including, where appropriate, through operation within a separate research enclave — rather than through relaxation of the applicable controls.

Ensuring robust security measures protects the University's digital ecosystem from threats and vulnerabilities. Devices lacking required security software or posing a threat to University IT Resources may be disconnected from the University Network without notice to prevent potential harm.

C. University-Owned Devices: University-owned Endpoint Devices remain University property at all times and may be recalled, restricted, restored, reimaged, reassigned, or retired in accordance with University procedures. Users are responsible for preserving the integrity, security configuration, management status, and operational condition of University-owned Endpoint Devices assigned to them. Access to User content on a University-owned Endpoint Device is governed by the User Privacy section of this policy.

Users must not intentionally damage, destroy, conceal, alter, wipe, reimage, dispose of, transfer, loan, sell, or otherwise make unavailable any University-owned Endpoint Device or component without Authorization. Users must not remove, disable, uninstall, alter, or interfere with University-installed or University-required software, operating systems, security tools, monitoring tools, management tools, logging capabilities, device-management enrollment, Encryption, access controls, or other required configurations except as expressly authorized under approved University procedures, an approved exception, or a documented research or instructional Authorization.

The University may remove unauthorized, altered, noncompliant, or potentially harmful software or configurations from University-owned Endpoint Devices; restore required software or configurations; restrict

access to University Networks or services; or take other reasonable action to protect the University, individuals, IT Resources, and University Data and ensure alignment with legal, investigatory, records, and compliance obligations. Where a security, legal, operational, or compliance risk is identified, such action may occur without prior notice. Any access to User content must comply with the User Privacy section of this policy.

Before taking action under this section that would result in the wiping, reimaging, reconfiguration, or reassignment of a University-owned Endpoint Device, the University will take reasonable steps to preserve research data, software, and other work product on the device, where feasible and consistent with the security, legal, operational, or compliance need giving rise to the action. Where circumstances permit, the University will coordinate with the affected User and, as applicable, the Office of Research Integrity, the Office of Research Security, the Office of the General Counsel, and the responsible department, to facilitate retrieval of such materials. Where the nature of the incident requires immediate action that does not permit advance coordination, the University will pursue as feasible the preservation of research data and work product through post-action recovery efforts.

D. Personally-Owned Devices: Personally owned Endpoint Devices used to access, create, transmit, store, or process University Data or University communications must meet University-defined security requirements appropriate to the device type and risk. These requirements may include current operating-system updates, device Encryption where supported, screen lock or biometric Authentication, non-rooted or non-jailbroken status, Multi-Factor Authentication, secure configuration, supported anti-malware or built-in platform security controls where applicable, and the ability of the User to preserve or remove University Data if the device is lost, stolen, compromised, replaced, or no longer used for University Operations.

Restricted University Data must not be downloaded, exported, copied, synchronized, stored, cached for offline use, or otherwise maintained on personally owned Endpoint Devices, personal accounts, or personally controlled services unless expressly authorized in writing under approved University procedures or an approved exception. Users may access Restricted University Data from personally owned Endpoint Devices only through University-approved services and only when the access method does not permit local storage, offline access, unmanaged synchronization, or other local retention of the Restricted University Data, unless expressly authorized. Routine transient technical caching necessary to display information in an approved service is not considered storage for this purpose, provided the User does not enable offline access, export, download, synchronization, or local retention.

Use of a personally owned device, personal account, or personally controlled service to create, send, receive, store, or access University Data or University communications may subject the University-related information on that device, account, or service to preservation, search, review, production, or disclosure under applicable Laws and Regulations, including the Rhode Island Access to Public Records Act, subpoenas, court orders, audits, investigations, and litigation discovery.

Receipt of a University stipend, reimbursement, or allowance for a personal device does not transfer ownership of the device to the University, does not grant the University general access to Personal Data, and does not waive privacy protections pursuant to Laws and Regulations. However, as a condition of using a personal device for University Operations, Users must cooperate with lawful and policy-authorized efforts to identify, preserve, collect, or produce University-related information. The University will endeavor to use the least intrusive means reasonably available and will follow applicable Laws and Regulations and institutional procedures.

Nothing in this section authorizes University personnel to access a personally owned device or unrelated Personal Data without the User's knowledge and consent, legal process, direction from the Office of

General Counsel or Human Resources, or documented exigent circumstances as described in the User Privacy section.

Users receiving a device stipend, reimbursement, or allowance may be required to acknowledge applicable security, records-preservation, public-records, investigation, and University Data obligations as a condition of receiving the stipend, reimbursement, or allowance.

Users are encouraged, and may be required where feasible, to segregate University Data and communications from Personal Data through reasonable means (e.g., separate applications, accounts, or profiles). Users are reminded that to the extent data or information is created, transmitted or stored while conducting University Operations on a personally owned Endpoint Device, such data and information may be deemed University Data subject to this and other University policies.

IV. University Email

The purpose of this section is to define the appropriate use, creation, and management of University issued email addresses and associated email domains (e.g., @uri.edu). It also ensures that email communications representing the University are consistent with institutional standards for branding, security, and official correspondence. It also establishes governance to prevent unauthorized use of University email resources.

This section applies to all University employees, faculty, students, University Affiliates, contractors, and any other individuals or entities granted access to University email systems or authorized to use email addresses under URI managed domains. This includes all primary and secondary email accounts that use the URI affiliated domains for University Operations, academic activities or sponsored programs.

A. User Responsibilities for Email Accounts: All Users of University email systems are responsible for:

- Using University issued email addresses (e.g., firstname.lastname@uri.edu) for official University-related communications, consistent with the personal-use provisions of Section I.G.
- Refraining from creating or using unauthorized email addresses that appear to represent the University or use URI owned domains without approval from the IT Security Office or the Division of External Relations and Communications.
- Maintaining the security of their University email account credentials and immediately reporting any suspected compromise.
- Following all University protocols and procedures related to email retention, Data Classification, and handling of protected or regulated data.
- Ensuring that email content reflects professional standards and complies with University policies and procedures, Laws and Regulations (e.g., FERPA, HIPAA, if applicable), and digital accessibility requirements.
- Not using automated means to forward University email to personal accounts or third-party providers unless explicitly permitted and properly secured, to maintain control over institutional communications and data.

Faculty and researchers may request authorization to forward University email to accounts at accredited academic or research institutions for purposes of sabbatical residency, multi-institutional research collaboration, or visiting appointments, provided the receiving institution maintains substantially equivalent security practices. Such arrangements shall be documented with the IT Security Office.

B. Permitted and Prohibited Email Activities: Users must use only University-provided email accounts to conduct University Operations. Use of personal email accounts to conduct University Operations is prohibited. University email may not be used for personal commercial activity, unauthorized solicitation,

political campaigning using University resources, or other activities that are unrelated to the University's mission or the User's University role. Additional limits may apply under Laws and Regulations, University policy, or University directives.

The following email activities are prohibited when using a University-provided email account:

- Sending an email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work-related purpose.
- Accessing the content of another User's email account, except: (1) at the request of the account owner for support purposes; (2) as required to respond to a documented information security incident or suspected incident; (3) as necessary to restore service continuity or recover University records for documented operational need; or (4) as required for public records requests, subpoena, legal hold, e-discovery, investigations, or other legal process. Such access must be authorized and documented in accordance with University procedures and the User Privacy section of this policy.
- Sending or forwarding any email that is known by the User to contain Computer viruses.

Emails that document University Operations are University records (University Data) and may be subject to applicable access to public records laws and records retention requirements. Incidental personal use may occur as permitted elsewhere in this policy; however, email stored or transmitted using University IT Resources may be subject to legal holds, public records requests, and other lawful access, and no expectation of privacy exists for such communications. Emails sent or received by Users while conducting University Operations are University Data that may be subject to applicable retention, access, and disclosure requirements.

V. Domain Names

The purpose of this section is to establish clear governance over the creation, registration, and use of all domain names and subdomains associated with the University's digital presence. It ensures that all subdomains under the primary URI domain (e.g., *.uri.edu) are managed in a manner consistent with the University's branding, security, accessibility, and strategic communication objectives.

All domain names and subdomains associated with the University's digital presence are considered the exclusive property of URI. This includes but is not limited to any domains registered under the primary URI domain.

The creation, registration, or use of any subdomain under the URI primary domain (e.g., subdomain.uri.edu) must receive prior written approval from the URI Division of External Relations and Communications. This approval process ensures consistency with brand, security, accessibility, and strategic communication goals.

Unauthorized registration or usage of subdomains is strictly prohibited and may result in the removal or reassignment of the domain.

VI. User Privacy

The University takes privacy rights and academic freedom seriously. University ownership or control of IT Resources, Access Credentials, accounts, data, hardware, or software does not authorize individual University personnel to access another User's data, communications, device, account, hardware, software, or system absent a legitimate institutional need and the approvals required by this policy and University procedures. Technical ability, administrative privileges, supervisory status, employment in ITS, HR, or any other University office, curiosity, or convenience is not Authorization.

Users are advised that there is no reasonable expectation of privacy regarding University-owned IT Resources, except to the extent required by Laws and Regulations or University policy. University-owned IT Resources are provided for institutional purposes and may be monitored or accessed as permitted by law and this policy. Any information or data stored or transmitted through University IT Resources or used in the performance of University duties may be subject to applicable access to public records laws, data retention requirements, and other potential public disclosure.

With respect to Personal Data that Users voluntarily choose to transmit or store through or with IT Resources, the University will, to the extent feasible and consistent with Laws and Regulations and University policy, respect the User's privacy rights and interests. However, Users do not have a reasonable expectation of complete privacy in such information, which may be accessed, monitored, or disclosed in accordance with University policies, legal obligations, and institutional operational needs.

If personal User data or communications are accessed or disclosed in a manner that violates this policy, the affected User shall have the right to an investigation and report of the incident. To the extent consistent with applicable law, this report will include an opportunity for the User to review any accessed information, an accounting of the individuals or processes involved, and a statement outlining the remediation steps taken to prevent future violations. If multiple individuals are affected, the University may, at its discretion, provide a consolidated report and statement to all affected parties.

Consistent with the University's commitment to academic freedom and research integrity, the University recognizes that research data, peer-review communications, pre-publication manuscripts, and communications with research subjects warrant heightened care. Such materials shall be subject to the heightened access standards in Section VI.A.3.

A. Monitoring and Inspection: The University aims to protect the integrity of its digital resources while maintaining trust and security within the community. Users may be subject to either or both of two distinct categories of monitoring on University Networks and IT Resources.

1. **Routine Monitoring:** Routine monitoring activity is necessary for security measures such as intrusion detection, resolving issues with network performance (e.g., speed, delays, and disruptions), and maintaining a healthy and secure network infrastructure. This practice is standard in higher education to ensure the safety and efficiency of University IT Resources. Routine monitoring may include:
    - Records of which devices connect to the University's networks and IT Resources.
    - Logs of user access to University IT Resources, including login times and accessed systems.
    - Records of websites visited by devices connected to University Networks.
    - Logs of data transfers and other significant network activities.

    Through device management software, University Network connections, and URI Systems, the University may access technical use information such as location logs, hardware and software usage, browser activity, and event history. The University has appropriate procedures to restrict access to this information, which may be used for security, investigation, diagnosis, and decision-making processes.

2. **Non-Routine Monitoring and Inspection:** Non-routine monitoring and inspection of data and communications will occur only when strictly necessary.

    Non-routine monitoring and inspection is permitted only under the written direction of the Office of General Counsel (OGC), or under emergency or exceptional circumstances. Emergency or exceptional circumstances may include, but are not limited to:
    - Responding to incidents where a University-owned device may be compromised.
    - Detecting and responding to cybersecurity threats or breaches.

- Addressing significant malfunctions or performance issues.
- Suspected fraudulent activities or legal, regulatory, compliance, or policy violations.
- Investigating reports of misuse or abuse of IT Resources.

Affected individuals will generally be informed in writing when practicable and consistent with the University's legal, operational, investigatory, and compliance obligations. Notice may be delayed, limited, or omitted when notification is prohibited by Laws and Regulations or other legal directive; when the non-routine monitoring and inspection is conducted as part of an ongoing investigation or is required for litigation, legal process, regulatory compliance, audit, or similar official purposes; or when notification is impracticable, infeasible, or would impose an unreasonable administrative burden.

Users with elevated privileges – namely, the technical capability to access other Users' data or communications – may have their activities monitored or inspected at any time without notice.

3. **Targeted Access to Individual User Content:** Targeted access to a User's content, communications, data, device, account, hardware, software, or system — beyond the routine and non-routine monitoring described above — is permitted only when one of the following applies:
    a. the User has knowledge of and consents to the access, such as for support;
    b. access is directed or approved by the Office of General Counsel, Human Resources, or another authorized University office for a documented legal, records, operational, security, compliance, or investigative need; or
    c. documented exigent circumstances require immediate access to protect people, preserve University Data or IT Resources, contain a security incident, restore critical service, or prevent loss or destruction of evidence or records.

    Access under exigent circumstances must be limited to the immediate need, documented promptly, and reported to the Office of General Counsel, Human Resources, the Security Office, or another appropriate office as soon as practicable. All access must be limited to the minimum necessary, logged where technically feasible, and handled in a way that respects privacy, academic freedom, legal obligations, and institutional need. Incidental access to personal or unrelated information must not be used or disclosed except as required by law, policy, or approved University procedure.

B. Safeguards and Oversight: The University recognizes the critical importance of safeguarding the community's research, teaching, and communication resources. To prevent potential abuse of access and control by IT personnel, the University will implement stringent internal processes, including but not limited to:

1. **Logging and Auditing:** All access to devices or IT Resources by authorized personnel will be logged to ensure transparency and accountability. Logs will include the identity of the individual accessing the information, the time and date of access, the specific information or resources accessed, and the purpose of the access. Whenever possible and to the extent it is reasonable, all activities involving access to Confidential or Restricted University Data or communications will be logged and subject to regular audits. Logs shall be secured with access limited to authorized Security Office personnel.
2. **Confidentiality Requirements:** All individuals with access to Confidential or Restricted University Data will be held to the highest standards of confidentiality.
3. **IT Governance Committee Oversight:** The IT Governance Committee, which includes faculty, student, and administrative staff representation, will oversee standards and compliance with these safeguards. This committee will provide an essential check and balance to ensure Security Office and community activities align with the University's commitment to academic freedom and privacy.

C. **Disclosure:** Disclosure of investigative results and of records created or maintained on University IT Resources is governed by Section I.H. Any access to User content in connection with disclosure or investigation must comply with the access requirements described in this section.

   The University will make every effort to protect User privacy to the extent feasible and consistent with Laws and Regulations, University policy, and operational need. Unauthorized Access by any University employee, including employees in ITS, HR, supervisory roles, administrative offices, or positions with elevated privileges, is a violation of this policy.

VII. Enforcement

Violations of this policy may result in disciplinary action, up to and including termination. Violators may also face additional sanctions or penalties imposed by the University and may be subject to penalties under Laws and Regulations 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 if found or suspected to be in violation of this policy. Measures may include eliminating access to networks, blocking external access to systems, blocking data transfer to or from Systems, and the physical seizure of hardware. Expedited access restrictions are initiated as described in Section I.I.

Any Unauthorized Access, disclosure, or misuse of Confidential or Restricted University Data will be met with serious repercussions, up to and including termination.

All violations will be documented in writing and kept on file for no less than three years. Administrators shall maintain documented standard operating procedures to ensure and enforce these measures.

Exceptions

Any exceptions to the provisions of this policy must be approved in writing by the Chief Information Security Officer (CISO). Such exceptions will be granted only under the most compelling circumstances and must be narrowly tailored to meet the stated need. Documentation of approved exceptions is required and must include:

1. The specific provisions being excepted.
2. The rationale for the exception.
3. The duration of the exception.
4. Any compensating controls implemented to mitigate associated risks.

For exception requests asserting a research, instructional, creative, or academic-freedom basis, the CISO may seek consultation with the IT Governance Committee as may be deemed appropriate. Final appeal lies with the CIO in consultation with the Provost and the Vice President for Research and Economic Development. A faculty member pursuing such an appeal may request that the Faculty Senate Committee on Technology and Infrastructure (“CTI”) submit input to the appeal reviewers. Where the faculty member makes such a request, the appeal reviewers will consider CTI's input as part of the appeal record.

Non-standard research devices and programmable embedded systems devices (such as Arduinos, FPGAs, and similar devices) that do not have full operating systems installed and cannot feasibly or reasonably comply with this policy's requirements are exempt, provided they do not access, process, or store Confidential or Restricted University Data. No written exception is needed under these conditions.

Research-specific hardware, such as medical devices that do not allow for software updates or other compliance measures, also do not require written exceptions but must be documented by sending the appropriate details to the IT Security Office at security@uri.edu. This documentation must include the rationale for non-compliance and any compensating controls implemented to mitigate associated risks.

Computers and comparable devices required to interface with research instrumentation or specialized equipment that cannot operate with current operating systems, current software versions, or standard security configurations may be authorized for continued use under a documented exception, with compensating controls appropriate to the circumstances, such as network isolation or segmentation, restricted data classifications, and physical access controls.

Research, instructional, testing, accessibility, repair, or specialized hardware that requires rooting, jailbreaking, reimaging, alternate operating systems, disabled controls, nonstandard security configurations, or similar modifications may be approved only through approved University procedures or an approved exception. Any approval must be documented, limited to the stated University purpose, identify the responsible User or unit, identify the device or class of devices, state the permitted modifications, specify permitted data classifications and network access, identify compensating controls, and include a review or expiration date where appropriate. Devices operating under such approval must not access, store, or process Confidential or Restricted University Data unless the approval expressly permits that use and documents the required compensating controls and approvals.

All exceptions will be reviewed periodically to ensure they remain necessary and that appropriate controls are in place.

Administrators must adhere to industry best practices for managing exceptions and maintain documented standard operating procedures to ensure and enforce these measures.

The CIO, CISO, and other designated University officials may issue, maintain, and update procedures, standards, approved-service lists, technical requirements, forms, acknowledgements, and guidance necessary to implement this policy. Such materials must be consistent with this policy and may be updated to reflect changes in law, technology, risk, University operations, and security requirements.

For device modifications in active research or instructional use as of the effective date of this policy, a one-time thirty (30)-day retrospective authorization window is provided during which responsible Users may submit documentation of existing configurations for review without penalty. This transition provision applies only to configurations in place as of the effective date and does not create an ongoing pathway for after-the-fact authorization.

Policy Review and Revisions

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

Policy #	Effective Date	Reason for Change	Changes to Policy
07.105.1	August 21, 2026	n/a	n/a

Note: This policy supersedes the following IT policies:

- Policy on IT Acceptable Use (07.103.2)
- Policy on IT Endpoint Protection (07.102.2)
- Policy on IT Resources (07.101.2)
- Policy on IT Service Protection (07.104.1)