Policy on Information Technology Data, Systems, and Services

[DRAFT DATE 20260409]

Policy Title	**Policy on Information Technology 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	_____
Next Review Date	No later than _____
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 that third-party service. **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 sensitive, protected, or confidential data is accessed, disclosed, or used by an unauthorized individual. **Data Classification.** Classifications as defined in the *URI Data Classification Schema and Guidelines*. Below are brief definitions for convenience; however, should the definitions change in the URI Data Classification Schema and Guidelines, those definitions shall prevail: ● **Public.** Information that is publicly available or, if disclosed, would cause no harm to URI or its community.

- **Internal.** Information that URI prefers to keep confidential but, if disclosed, would cause only minor damage.
- **Confidential.** Information for which disclosure would cause significant damage to URI or its community. Such as FERPA, HIPAA, and other protected data. This also includes sensitive business information that is valuable to the University.
- **Restricted.** Information for which disclosure could result in major and possibly irreparable damage to URI or its community. This includes highly sensitive business information that is protected by statutory, regulatory, and/or contractual requirements Restricted Data includes data designated as Controlled Unclassified Information (CUI) under federal regulations and any data requiring security clearance.

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 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.

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.

Phishing. A type of cyber attack in which an attacker sends a fraudulent message designed to trick a person into revealing sensitive information, gaining unauthorized access, or deploying malicious software.

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 data.

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

Service Level Agreement (SLA). A contract between a service provider and a customer that specifies the expected level of service, performance metrics, and responsibilities.

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 provided by external vendors or contractors that are used by the University to support its IT infrastructure and operations.

Two-Factor Authentication (2FA). A special case of multi-factor authentication; a method of confirming a User's identity by utilizing two different types of information, typically something the User knows (password) and something the User has (security token).

Unauthorized Access. Any access, use, entry, or attempt to access, use, or enter any system or systems, 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 business, 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, academic or student affairs, research, or other University activities, 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 data (e.g. FERPA, HIPAA, research, personnel, and other protected data) are included. ● **Personal Data:** Personal data that does not relate to University business but 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 applicable 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. **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	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.

Policy	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 (Identity Theft Protection Act of 2015). R.I.G.L. § 5-37.3 et seq. (Rhode Island Confidentiality of Health Care Communications and Information Act). Payment Card Industry Data Security Standard (PCI DSS). *Policy on Conflict of Interest and Commitment*.
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 and IT Users; 3) require appropriate protections on all Endpoint Devices used for University business; 4) define the responsibilities of Administrators to protect and secure IT Resources; and 5) comply with state and federal law.
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, the security of all community members, and compliance with state and federal law. Concurrently, URI is committed to the foundational principles of academic freedom and privacy, and recognizes that these are essential to fostering an environment of intellectual exploration, innovation, and rigorous scholarship. The University is dedicated to maintaining a judicious balance between the dual imperatives of safeguarding Information Technology ("IT") Resources and preserving academic freedom and privacy.

All IT Users ("Users") must comply at all times with 1) applicable local, state, federal, and international laws, regulations, and ordinances; 2) University policies and ethical codes; 3) contractual obligations; and 4) reasonable best practices.

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 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 or contracts between the University and any covered parties, or any applicable ordinances, laws, regulations, or any University Board of Trustees policy that conflict with this policy. In the event of any such conflict, the terms of the collective bargaining agreements, contracts, ordinances, laws, 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, 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-related business, educational, and academic pursuits, as well as business operations;
2. Respect the privacy interests of other Users and adhere to University 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. Circumvent University IT security measures.
3. Engage in activities contrary to the University's mission(s) or applicable laws and regulations.
4. Send unsolicited messages to a large number of recipients ("spamming").
5. Consume an unauthorized disproportionate share of networking resources (e.g., misuse of peer-to-peer applications).
6. Deliberately cause any denial of service, including flooding, ICMP attacks, or the unauthorized automated use of a service intended solely for human interaction.
7. 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.
8. Engage in excess use of IT Resources, allowing entry to non-public hosts, tampering with security measures, performing any illegal acts through IT Resources, violating others' privacy, or the use of IT Resources to libel, slander, or harass others.
9. Access protected resources without authorization, including another User's account or private data.

C. Training Requirements: All Users, including faculty, staff, students, and University Affiliates, must successfully complete annual security awareness training. Additionally, those who manage sensitive data must also take and pass annual domain-specific training, such as FERPA, HIPAA, Payment Card Industry (PCI), or other relevant training. Users administering systems (generally IT professionals) 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: Documents, data, and other materials that support University operations, decision-making, or compliance obligations, or that are subject to legal, regulatory, or records retention requirements, must be stored in University-approved, shared, or centrally managed repositories designated for that purpose.

Individual user storage locations are not appropriate systems of record for such materials, even when those locations are provided by the University. 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, or shared function. If it lives in one person's account, it is not an acceptable system of record, even if the service is University-provided.

Materials stored solely in an individual User's account may become inaccessible or be deleted when that account is deactivated, when the individual changes roles, or when the individual separates from the University, and must not be relied upon as the sole location for University records or operationally essential documents.

Users are responsible for ensuring that University records and essential operational documents are stored in shared, role-based, or departmental repositories in accordance with applicable University records management policies and procedures.

E. Confidentiality and Security of Data: Users must access University Data solely for conducting University business and only as permitted by applicable confidentiality and privacy laws, contracts, and policies. This ensures the integrity and security of URI's digital infrastructure while upholding the University's commitment to privacy 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 State of Rhode Island record retention schedules, federal and contractual data retention requirements, and University policies to comply with legal obligations and support institutional accountability.

Users are prohibited from using any unapproved third-party application, platform, service, or tool (no matter how obtained) to create, store, transmit, process, or handle Confidential and/or Restricted data. This prohibition applies to student records protected under FERPA, protected health information (HIPAA), Confidential or Restricted research data, personnel records, and other protected data. 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 data.

1. **Handling of Confidential Data:** Confidential University Data or any data classified as Confidential or Restricted must not be accessed, used, or disclosed without prior authorization from a designated University official with documented authority and an articulated institutional need. This protects the privacy and security of sensitive information, aligning with the University's commitment to safeguarding intellectual exploration and innovation. When sharing Confidential University Data, Users must ensure that recipients are authorized to receive such information. Confidential 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 protecting vendor information, such as software code and proprietary methodologies, to honor contractual obligations and maintain trust.
2. **Requests for Access to Confidential Data:** Offices that may handle requests for Confidential 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 University Data must be authenticated and approved by the Office of General Counsel or the Director of Records Management. All such requests must be documented, tracked, and maintained according to the appropriate retention schedule, with an official recorded approval method, to ensure a clear audit trail and accountability.
3. **Data Storage and Encryption:** Confidential University Data must be stored on centrally managed or contracted IT Resources, not on local hard drives or portable devices, unless prohibited by law or

binding agreement. This centralization enhances data security and ensures compliance with institutional policies. Additionally, Confidential University Data must be encrypted during transmission over a network and while stored to protect against unauthorized access and data breaches. Unauthorized disclosure or suspicion of unauthorized access to Confidential University Data must be reported to the Security Office (security@uri.edu) within two hours of becoming aware of the incident to enable prompt response and mitigation.

4. **Security Software and Practices:** 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. 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.

   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.

5. **Use of Commercial Cloud Services:** Non-enterprise End User License Agreements (EULAs) and similar agreements (collectively referred to as "Digital Agreements") that Users agree to when accepting the terms and conditions of 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 entering into such agreements. It is the sole responsibility of the User to ensure full compliance with this policy before agreeing to any terms and conditions.

   Every IT User must understand the contents 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, and legal liabilities. Additionally, EULAs and similar agreements may extend legal liabilities to the Users or the University or significantly limit the legal rights of either.

   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). If no approved service is available, Users may use an alternative service only with written acknowledgment that no data above "Public" will be stored, or, with prior written approval from the Security Office, data classified as "Internal." Data classified as "Confidential" or "Restricted" may not be stored in unapproved services.

6. **Email:** Users must use only University-provided email accounts to conduct University-related business. Use of personal email accounts to conduct University business 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 applicable law, 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; (3) as necessary to restore service continuity or recover University records for documented operational need; or (4) as required for APRA, subpoena, litigation hold, e-discovery, or other legal process. Such access must be authorized and documented in accordance with University procedures.
- Sending or forwarding any email that is known by the User to contain computer viruses.

Emails that document University business are University records (University Data) and are subject to applicable 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 business are University Data that are subject to access to public records laws, state records retention and security requirements.

7. **Security and Use of Remote Services:** All electronic devices, including personal computers, phones, or other devices used to access, create, or store University IT Data or IT Resources, including email, 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 multifactor authentication (MFA) methods.

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

   If University Data is created or stored on a User's personal computer or other device, or in databases that are not part of the University's IT Resources, this data and these devices are subject to Public Information Requests, subpoenas, court orders, litigation holds, discovery requests, and other requirements applicable to University IT Resources.

8. **Access of Accounts and Sharing of Credentials:** 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.

   Passwords, personal identification numbers (PINs), digital certificates, security tokens, or similar information or devices used by Users for identification and authorization purposes (collectively "Access Credentials") while using University IT Resources 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.

   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 designee, must be documented, time-limited, and scoped to the minimum access necessary, and must follow the procedures outlined in the accompanying Procedures document.

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, regulations, and University policies. Both the owner of the Access Credentials and the individual granted access can be held responsible for violations of this section of the policy or failure to follow related procedures.

9. **Use of Copyrighted Materials:** The University is committed to upholding U.S. copyright laws, which protect copyrighted materials. All Users are prohibited from violating 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 has been granted by the copyright owner.

   Please note that this information is provided for general guidance and should not be construed as legal advice. In cases of uncertainty or specific questions about copyright law and its application, Users can consult the Office of General Counsel to ensure compliance with legal requirements.

F. 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 activities or violate University policies. 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 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.

   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.

   Supervisors, appropriate offices, applicable University policies, or state laws 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.

G. 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 General Counsel (OGC). Communications created with University IT Resources may also be subject to Rhode Island's Public Records statutes. Users may be subject to legally binding demands such as subpoenas and search warrants.

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 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 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 sensitive data and 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 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. Under no circumstances should individuals who are not normally authorized and do not customarily have access 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 Information 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 should be limited to the necessary functions and permissions required for the user's role. All privileged access must employ Multi-Factor Authentication (MFA) 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.

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.

III. Endpoint Protection

The purpose of this section is to establish rules and guidelines for securing and managing endpoint protections on University-owned devices and personally owned devices used for University business, 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, and guests. It covers IT Resources administered centrally, by individual colleges or departments, and includes personally owned devices connected to all University networks, both on-campus and remotely.

B. User Responsibilities: IT 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 business, whether University-owned or personally owned, must not be used for malicious or illegal activities.

All devices must be kept fully patched and up to date. The University will assist with automatic patch installation for University-owned devices (contact ITS Service Desk for assistance). Users must not tamper with or uninstall any management or security software installed by the University.

C. University-Owned Devices: Devices provided by the University remain URI property and can be revoked or reassigned. All devices must be returned upon separation from the University or when a new device is provided. The University may remove unauthorized, altered, or potentially harmful software from University-owned devices to protect the University, people, systems, data, or meet compliance obligations. In certain circumstances where a risk is identified, removal may occur without prior notice. Personal data creation and retention must not impede device functionality or violate laws. When traveling internationally, Users must adhere to procedures and guidelines on foreign travel and export controls.

D. Personally-Owned Devices: Personal devices accessing University networks or URI services must have active and updated anti-virus and anti-malware applications. Jailbroken or rooted devices are not permitted. The University reserves the right to deny access to non-compliant devices.

Personal devices used for University business must allow the User to remotely wipe all data in the event the device is lost, stolen, or compromised. Users are responsible for backups and must provide access when required for legal or investigative purposes.

Users are advised to utilize University-owned devices to conduct University business whenever feasible. If personally-owned laptops or desktops must be utilized for University business, Users must install University-provided monitoring and security software, use multifactor authentication (MFA), and employ unique identities with strong passwords or biometric verification.

IV. University Email

The purpose of this section is to define the appropriate use, create, and management of University issued email addresses and associated email domains (e.g., @uri.edu). It also ensures that email communications representing

the University of Rhode Island (URI) 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, 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 official University business, academic activities or sponsored programs.

All users of University email systems are responsible for:

- Using University issued email addresses (e.g., firstname.lastname@uri.edu) solely for official University related communications.
- Refraining from creating or using unauthorized email addresses that appear to represent the University or use URI owned domains with approval from University ITS orthe 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 sensitive or confidential information.
- Ensuring that email content reflects professional standards and complies with University policies, applicable laws (e.g., FERPA, HIPAA, if applicable), and digital accessibility requirements.
- Not forwarding University email to personal accounts or third-party providers unless explicitly permitted and properly secured, to maintain control over institutional communications and data.

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 and academic freedom seriously and implements safeguards to protect personal and academic data. Nonetheless, Users are advised that there is no legal expectation of privacy regarding University-owned IT Resources. The University shall uphold privacy protections as required by law. Any data stored or transmitted through University IT Resources or used in the performance of University duties is likely subject to the Freedom of Information Act (FOIA) and the Rhode Island Access to Public Records Act (APRA) requests, data retention requirements, and 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, endeavor to respect the User's privacy interests in the information. However, Users may have no expectation of complete privacy in such information, which is subject to the same University access and monitoring practices as other University Data.

If 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. 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.

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.

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 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 generated by faculty, staff, or students 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 be informed in writing unless the action is part of an ongoing investigation or notification is prohibited by law or court order.

    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.

B. Safeguards and Oversight: The University of Rhode Island 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 data or communications will be logged and subject to regular audits. Logs shall be secured with access limited to authorized ITS personnel.
2. **Confidentiality Requirements:** All individuals with access to Confidential or Restricted 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 ITS and community activities align with the University's commitment to academic freedom and privacy.

C. 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 General Counsel (OGC). Communications created with University IT Resources may also be subject to Rhode Island's Public Records statutes. Users may be subject to legally binding demands such as subpoenas and search warrants.

Except where strictly not possible, legally required, or as otherwise authorized or directed by the Office of General Counsel (OGC), only data without information capable of identifying individual Users shall be accessed or disclosed.

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 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 if found 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.

Any unauthorized access, disclosure, or misuse of Confidential or Restricted data will be met with serious repercussions, including possible 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 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.

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 section'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, do not require written exceptions but must be documented by sending the appropriate details to security@uri.edu. This documentation must include the rationale for non-compliance and any compensating controls implemented to mitigate associated risks.

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.

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	_____	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)