THE
UNIVERSITY
OF RHODE ISLAND

Policy on IT Service Protection

Policy Title	**Policy on IT Service Protection**
Policy #	07.104.1
Policy Owner	Chief Information Officer
Contact Information	Questions regarding this policy should be directed to the Chief Information Officer at (401) 874-4599
Approved By	Administrative Policy Committee
Effective Date	June 7, 2022
Next Review Date	No later than June 30, 2027
Who Needs to Know About this Policy	All individuals who administer University servers, Systems, services or are responsible for third-party services that handle University Data or provide a software/IT Service to the University of Rhode Island.
Definitions	**Administrator**. Any individual who administers Systems, servers, and services and anyone designated as responsible for third-party services **IT Resources**. All computer and telecommunications equipment, software, data, and media, owned or controlled by University or maintained on its behalf. **IT Service**. All software and hardware components that together support a multi-user environment supporting any aspect of URI operations including teaching, research, service, or administration. **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. **University Data**. All data or information held on behalf of the University of Rhode Island, created as a result and/or in support of University business, or residing on University IT Resources, including both electronic and paper records. University Data includes personal data (e.g., personal emails to friends, copies of tax returns) of Users that do not relate to University business but that Users voluntarily choose to transmit or store on IT Resources.

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

Policy Statement

University of Rhode Island-owned servers, Systems, and third parties together provide vital IT Services to the University of Rhode Island (also, "University"). Administrators of such Systems and services must meet stringent standards that safeguard University Data, protect University-owned IT Resources, and in general support the prevention of disruption to any University business supported by such Systems and services. When a third-party is involved, a University staff member must be designated as responsible for evaluating the fitness of the third-party's products and services with respect to the standards of protection and safeguarding, as detailed in the following sections.

Applicability

This policy applies to all Systems, servers, and services that handle University Data or provide a software/IT Service to the University, and their Administrators and any staff designated as responsible for third-party services (collectively, "Administrators.")

Inventory and Status

Administrators must maintain a current list of Systems for which they are responsible. For each System, they must maintain documentation about its:

1. Name and purpose
2. Physical location
3. Name(s) of software installed
4. The nature of any University Data handled or stored
5. The volume of University Data

Additionally, with respect to the following standards, the status of these Systems must be periodically reviewed, documented, and dated. The frequency of this review must be commensurate with the sensitivity of data and/or how critically dependent the University is on the System, and the frequency cannot be less than once per year.

Third-Parties

Where Systems are controlled by a third-party, Administrators must have positive affirmation from the third-party, such as with through published policies and/or other written documentation, of meeting the following standard. This affirmation is commonly documented through the use of the Higher Education Cloud Vendor Assessment Tool (HECVAT), completed by the vendor at the time of purchase. In addition, Administrators must maintain records of both the nature and volume of University Data stored on these Systems.

Data and Systems

Administrators must take measures to prevent the loss, theft, or ransoming of University Data and disruption to University functions and servers. Examples of such measures may include full log capture, System intrusion detection, System hardening measures, and others as defined by IT Security.

All nonpublic-facing University Data must be encrypted at rest and encrypted in transit to prevent the unauthorized access to such data, such as by theft or electronic interception.

All University Data must be backed up, at a frequency determined to be acceptable and commensurate with the nature of data. Backups must be (1) encrypted, (2) physically distant from the primary copy, (3) protected against ransomware, and (4) require Multi-Factor Authentication (MFA) for access.

All Systems must be backed up or made otherwise recoverable should the System be destroyed or otherwise rendered inoperable. This standard can be achieved, for example, with full-disk snapshots, virtual machine imaging, scripted recreation of the server, or participation in disaster recovery services.

Network Security

Network access to Systems must be protected, such as by firewalls, to allow access to the Systems only to those network locations and entities that need such access to function.

Physical Security

Where Systems are on-premise or otherwise under the University’s direct physical control, they must be housed in a locked room where physical access is (1) controlled, such as with physical keys, electronic locks, and/or other devices restricting physical access, (2) logged, such as with a logbook or electronic records, and (3) monitored with video surveillance.

Privileged Access

Privileged access to Systems must be limited to the smallest number of people that is practical, but at least two (2), for the purpose of redundant staff coverage. Where possible, privileged access must be tailored to only the functions and permissions required by the activity of the accessing party. All privileged access must employ Multi-Factor Authentication (MFA), where supported. Systems that do not support MFA must gain special University approval for use and, if approved, must have other security elements that mitigate the lack of MFA. Access to Systems must be revoked when someone should no longer has access, and the Administrator must periodically review all accounts and remove any that are no longer used; the frequency of review is commensurate with the sensitivity of the System and University Data, and the frequency cannot be less than once per year.

Monitoring and Security Software

Where applicable, Systems must have University-approved anti-virus, security, and monitoring software installed, for the purpose of protecting University Data and Systems. All Systems must have full logging enabled for all security-related events within the System.

Policy Enforcement

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

The University may restrict or deny access to any University IT Resource temporarily or permanently to any service delivery mechanism found to be in violation of this policy, including eliminating access to the networks, blocking external access to the System, blocking data transfer to or from other Systems, and physical seizure of hardware.

Exceptions

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

Policy Review and Revisions

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

Policy #	Effective Date	Reason for Change	Changes to Policy
07.104.1	June 7, 2022	n/a	n/a