Policy 4-004: University of Utah Information Security Policy

Revision 5. Effective date: September 12, 2023

I. Purpose and Scope

A. Purpose

The purpose of the Information Security Policy is:

1. to establish the University of Utah (University) Information Security Program;
2. to ensure compliance with all applicable federal, state, and local laws, regulations, and statutes, as well as contractual obligations;
3. to ensure the protection of the University Information Assets, Information Systems, and IT Resources from Unauthorized Access or damage; and
4. to maintain the confidentiality, integrity, and availability of Information Assets and Information Systems supporting the mission and functions of the University.

B. Scope

The scope of this policy is all University administrative units, including colleges, divisions, departments, and centers, and all members of the University community, including students, staff, faculty, other permanent or temporary employees, contractors, research collaborators, vendors, and third-party agents. Compliance with this policy, and all its related rules and procedures, is compulsory for any group or individual in the scope of this policy.

II. Definitions

The following definitions apply for the limited purposes of this policy and any associated regulations.

A. Account – A login ID in combination with a password, passphrase, PIN, or other authentication token used to access any University Information System, Electronic Resource, or IT Resource.

B. Account Provisioner – An IT Technician who is responsible for the creation, management, and maintenance of User rights and privileges, objects, and attributes in relation to accessing Information Systems, Information Assets, Electronic Resources, and IT Resources.

C. Application – Any individual or standalone piece of software that provides a specific service to a community of Users or acts as an interface to an Information System.

D. Asset – Any University-owned Information Asset or IT Resource that is a part of University business processes.

E. Change – An event or action that modifies the configuration of any component, Application, Information System, or service.

F. Control – A means of managing Risk. A Control can include policies, rules, procedures, processes, practices, or organizational structures, which can be of an administrative, physical, or technical nature.

G. Electronic Communication – A means for exchanging digital messages. This includes, but is not limited to, email, Teams, Zoom, etc.

H. Electronic Resource – Any technology used for Electronic Communication. This includes, but is not limited to, internet, email, and social media.

I. Encryption – The alteration of information using a code or mathematical algorithm so as to be unintelligible to Unauthorized Access.

J. Information Asset – Data or knowledge stored in any electronic manner and recognized as having value for the purpose of enabling the University to perform its business functions.

K. Information System – An IT Resource used to electronically create, store, process, or transmit any University data or Information Asset.

L. Information System Media – A device on which an Information System's Information Assets are stored for backup and recovery purposes (e.g., backup tapes, backup disks, network attached storage/storage area network drives, magnetic media).

M. Intellectual Property – Any intangible Asset that consists of human knowledge and ideas (e.g., patents, copyrights, trademarks, software).

N. IT – Information Technology

O. IT Resource – A Server, Workstation, Mobile Device, medical device, networking device, web camera, monitoring device, or other device/resource that matches one or more of the following criteria:

1. owned by the University;
2. used to conduct University business regardless of ownership;
3. connected to the University's network; or
4. creates, accesses, stores, or transmits Information Assets.

P. IT Security Incident – An event or weakness that jeopardizes the confidentiality, integrity, or availability of the University's Information Assets, IT Resources, or Information Systems.

Q. IT Technician – Any University employee who develops, administers, manages, and monitors the IT Resources, Information Systems, and Electronic Resources that support the University's IT infrastructure, including UIT/ITS employees and employees of other University units.

R. Log – A chronological sequence of system activities and records which contains evidence directly pertaining to and resulting from the execution of a business process or system function.

S. Mobile Device – A portable, handheld electronic computing device that performs similar functions as a Workstation (e.g., iPhone, Android phone, Windows phone, Blackberry, Android tablet, iPad).

T. NIST – National Institute of Standards and Technology

U. Patch – A fix to a program failure, bug, or Vulnerability. A Patch may also be referred to as a Service Pack.

V. Remote Access – Access to Information Assets from any location outside of the University's network or physical boundaries.

W. Restricted Data – Any type of data classified as Restricted per Rule R4-004C.

X. Risk – The likelihood of a Threat agent taking advantage of a Vulnerability and the corresponding business impact. Risk is usually calculated as either a quantitative or qualitative score, and can be represented in the following equation: Risk = (Likelihood of Threat/Vulnerability Event Occurrence) X (Business Impact of Event Occurring).

1. Inherent Risk – The likelihood and impact of loss resulting from lack of action, either purposeful or not.

2. Residual Risk – The Risk that remains after Controls or other mitigating factors have been implemented for an environment, IT Resources, Information System, or Electronic Resource.

Y. Security Baseline – The minimum cybersecurity Controls needed to protect the confidentiality, integrity, and availability of Information Assets stored, processed, or transmitted on an IT Resource or Information System.

Z. Sensitive Data – Any type of data classified as Sensitive per Rule R4-004C.

AA. Server – The hardware and software used to provide information and/or services to multiple Users.

BB. Threat – Anything (human, natural, or environmental) that has the potential to cause harm.

CC. Unauthorized Access – Entry into any IT Resource, network, storage medium, system, program, file, User area, controlled physical area, or other private repository without the permission of the steward or owner.

DD. User – Any person, including students, staff, faculty, permanent and temporary employees, contractors, vendors, research collaborators, and third-party agents, who accesses any University Electronic Resources, Information Systems, and/or IT Resources.

EE. Vulnerability – A weakness that could be used to endanger or cause harm to an Asset.

FF. Workstation – An electronic computing device, terminal, or any other device (e.g., desktop computer, laptop, Windows tablet) that performs as a general-purpose computer equipped with a microprocessor and that is designed to run commercial software (such as a word processing Application or internet browser).

III. Policy – Roles and Responsibilities

A. University administration is responsible for:

1. supporting IT security through vision, clear direction, and demonstrated commitment of resources.

B. Executive University Information Technology (UIT)/Information Technology Services (ITS) leadership is responsible for:

   1. evaluating and accepting IT security Risk on behalf of the University;
   2. defining IT security responsibilities and goals and overseeing their integration into relevant processes;
   3. defining processes for determining information classification and categorization based on industry-recommended practices, University directives, and legal and regulatory requirements in order to determine the appropriate levels of protection for that information;
   4. defining processes for Information Asset identification, handling, use, transmission, and disposal based on information classification and categorization;
   5. the confidentiality, integrity, and availability of Information Assets;
   6. participating in the response to IT Security Incidents;
   7. complying with notification requirements in the event of a data breach;
   8. adhering to specific legal and regulatory requirements related to IT security;
   9. communicating legal and regulatory requirements to the Information Security Office; and
   10. communicating the requirements of this policy and its associated procedures, and the consequences of noncompliance to Users and third parties, and addressing adherence in third-party agreements.

C. The Chief Information Security Officer is responsible for:

   1. developing the IT security program and strategy, including measures of effectiveness;
   2. establishing and maintaining enterprise IT security policy and procedures;
   3. assessing compliance with IT security policies;

4. directing IT Security Incident response coordination and applicable remedial response efforts;

5. the Information Security Office staff, and any other IT Technician or IT manager performing IT security functions on behalf of the University; and

6. serving as the department head of the Information Security Office, which is responsible for:

   a. assessing University compliance with IT security policies, procedures, and legal and regulatory IT security requirements;

   b. evaluating and understanding IT security Risks;

   c. ensuring IT security architecture considerations are addressed;

   d. advising on IT security issues related to procurement of products and services;

   e. disseminating Threat information to appropriate parties; and

   f. promoting IT security awareness.

D. IT managers are responsible for:

1. providing resources needed to maintain IT security Controls consistent with this policy and related regulations;

2. providing IT Technicians with resources needed for training applicable to their area of responsibility;

3. implementing, in their area of responsibility, all University IT security policies, procedures, and processes as defined by executive UIT/ITS leadership; and

4. implementing business continuity and disaster recovery plans.

E. IT Technicians are responsible for:

1. implementing IT security Controls consistent with this policy and related regulations;

2. actively monitoring for issues which may impact the confidentiality, integrity, and availability of the Information Assets which are stored, processed, or transmitted on IT Resources, Information Systems, or Electronic Resources;
3. ensuring that IT security-related activities are well-documented and completed in a consistent and auditable manner;
4. in some cases, serving in the role of Account Provisioner;
5. working with the Information Security Office to resolve issues which impact the confidentiality, integrity, and availability of Information Assets; and
6. maintaining IT and IT security training, as relevant to assigned duties by IT managers.

F. Users are responsible for:

1. following this policy and related regulations;
2. complying with Utah System of Higher Education Policy R345: Information Technology Resource Security and R840: Institutional Business Communications;
3. complying with applicable federal and state laws; and
4. reporting suspected IT Security Incidents or Vulnerabilities to their respective help desk.

IV. Policy

A. Acceptable Use

University IT Resources, Information Systems, and Electronic Resources shall be used for legitimate patient care, instructional, research, administrative, public service, and approved contract purposes. Limited personal use of IT Resources, Information Systems, and Electronic Resources may be authorized if the use does not interfere with University duties or violate the terms of any University regulations. If University IT Resources are used for personal use, within the bounds of this policy, the University is under no obligation to provide support for that use.

1. IT Resource and Information System
   a. Users shall:
      i. use only the University IT Resources and Information Systems that they are authorized to use and use them only in the manner and to the extent authorized; and
      ii. comply with all federal, state, and other applicable laws; all applicable University regulations; and applicable contracts and licenses. Users are responsible for knowing, understanding, and complying with the laws, policies, rules, procedures, contracts, and licenses applicable to their particular uses.
   b. Users may not:
      i. attempt to circumvent the IT security mechanisms of any University IT Resource or Information System as established by the Information Security Office;
      ii. attempt to degrade system performance or capability; or
      iii. attempt to damage IT Resources, Information Systems, software, or Intellectual Property of others.
2. Account Use
   a. Users may not:
      i. share an Account, username, password, and/or any other authentication token or use another User's Account, username, password, or other authentication token; or
      ii. view or use another User's Accounts, computer files, programs, or data. Access to such information does not imply permission to view or use it.

3. Electronic Resources

   a. Users shall:

      i. use Electronic Resources for purposes consistent with the University's values, policies, and applicable rules and procedures;

      ii. protect access to and the integrity of Electronic Resources;

      iii. abide by local, state, federal, and applicable international laws, contractual obligations, regulations, and University regulations; and

      iv. use Electronic Resources only for their appropriate purpose.

   b. Users may not:

      a. infringe on the Intellectual Property rights, privacy, or personal rights of others.

4. Intellectual Property Use

   a. Users shall:

      i. only install or distribute software on University Information Resources that is appropriately licensed for use by the University; and

      ii. abide by federal copyright laws when using University IT Resources and Information Systems for the use or copying of copyrighted material. The unauthorized publishing or use of copyrighted material on University IT Resources and Information Systems is prohibited, and Users are personally liable for the consequences of such unauthorized use.

   b. Users may not:

      i. violate the rights of any person, organization, or company protected by trade secret, patent, Intellectual Property rights, or similar laws or regulations.

For more specific requirements, please access Rule R4-004A.

B. IT Security Risk Management

1. The University's IT Security Risk Management Program (the Program) shall support the University's business missions by doing the following.

   a. The Program shall secure the Information Systems that create, store, process, or transmit the University's Information Assets. The University primarily uses the CIS 18 Control framework, however, depending on regulatory and contractual obligations, other government and industry-recognized frameworks may be required. Please contact iso-grc@utah.edu or ciso@utah.edu with questions.

   b. The Program shall issue both Inherent and Residual Risk scores in Risk assessment summary reports for all Information Systems assessed to the cognizant vice president, dean, or other person in a position of similar seniority able to accept Risk on behalf of the University. These individuals shall be responsible for either formally accepting the Risk of operating the Information System in the University's environment or rejecting the Risk and requiring a formal corrective action plan to allocate the appropriate timelines, budget line items, and/or other resources to remediate Control failures and reduce the Residual Risk score to an acceptable level for the University. Users, IT Technicians, and IT managers are not authorized to accept risk for the University of Utah.

   c. The Program collaborates with other University Risk management activities to ensure the priorities of the University's IT security program priorities are aligned appropriately with the University's Risk tolerance.

   d. The Program provides a systematic methodology to assess and manage IT security Risk for the University. The University's methodology is based foremost on NIST SP 800-30, "Risk Management Guide of Information Technology Systems."

C. Data Classification and Encryption

1. The University shall protect Restricted and Sensitive Information Assets that are created, stored, processed, or transmitted using IT Resources and Information Systems. IT Technicians shall establish, document, implement, and manage data handling and management procedures for the IT Resources and Information Systems they support.

    a. Data Classification: All Information Assets shall be classified in accordance with Rule R4-004C.

    b. Data Handling: All Information Assets shall have appropriate handling procedures in accordance with their data classification.

    c. Encryption: All Information Assets shall have Encryption requirements in accordance with their data classification.

For more specific implementation requirements, please access Rule R4-004C.

D. Access Management

1. Only authorized Users shall have physical, electronic, or other access to IT Resources, Information Systems, Information Assets, and Electronic Resources. Access shall be limited to Users with a business need to know and dependent on the requirements of their job functions. It is the shared responsibility of IT Technicians and Users to prevent Unauthorized Access to IT Resources, Information Systems, Information Assets, and Electronic Resources. IT Technicians shall implement access Controls which include effective procedures for granting authorization, tools, and practices to authenticate authorized Users and to prevent and detect unauthorized use.

    a. Account Authorization: University Accounts shall be issued after the request is authorized appropriately and documented adequately.

    b. Account Authentication: University Accounts shall be authenticated at a minimum via unique login IDs, complex passwords or passphrases, and multifactor tokens.

c. Account Termination: University Accounts shall be deactivated, disabled, and/or deleted immediately upon termination of contract, employment, or relationship with the University.

d. Account Reaccreditation: Account Provisioners shall conduct periodic reviews of authorized accounts.

e. Certain events may require that a User's access rights be immediately removed. In these situations, as directed by the cognizant authority, the User's rights will be revoked, and the respective help desk notified immediately.

For more specific implementation requirements, please access Rule R4-004D.

E. Change Management

Any Changes to University IT Resources and Information Systems in service that store, process, or transmit Restricted or Sensitive Data shall be authorized, tested, documented, and approved by IT managers prior to implementation.

1. Separation of Duties

   a. Account Provisioners shall ensure that no single individual can modify University IT Resources and Information Systems without authorization.

2. Separate Environments

   a. IT Technicians shall physically, logically, or virtually separate test, development, and production environments to reduce the Risk of unauthorized Changes to University IT Resources and Information Systems.

F. Physical and Facility Security

1. IT managers and IT Technicians shall physically protect IT Resources and Information Systems they are responsible for against natural and environmental Threats by:

a. planning and implementing Controls for safeguarding physical components against compromise and environmental hazards; and

b. installing, in data centers and sites where Information Systems and IT Resources are located, locks, cameras, alarms, redundant power systems, fire detection and suppression systems, access Controls, and other safeguards as applicable to ensure protection from natural and environmental Threats and to respond to Unauthorized Access to electronic or physical components contained in these areas.

For more specific implementation requirements, please access Rule R4-004F.

G. IT Resource and Information System Security and Vulnerability Management

1. All IT Technicians, IT managers, and Users managing University IT Resources, Information Systems, and Electronic Resources shall:

a. protect any IT Resources and Information Systems under their management from compromise;

b. configure IT Resources and Information Systems to reduce Vulnerabilities to a minimum and apply all relevant IT security Patches to fix IT security issues;

c. use the Information Security Office (ISO)-approved systems for antivirus/anti-malware, endpoint detection and response (EDR), data loss prevention (DLP), and privilege management;

d. utilize Security Baseline settings to ensure IT Resources and Information Systems are available for use and guarded against malware and/or other forms of compromise;

e. periodically verify Logs, examine performance data, and generally check for any evidence of Unauthorized Access, viruses, or other malicious code; and

f. cooperate with the Information Security Office by providing support for and/or review of administrative activities, as well as performing more sophisticated procedures, such as penetration testing and real-time intrusion detection.

For more specific implementation requirements, please access Rule R4-004G.

H. Remote Access

1. IT Technicians who grant Remote Access privileges and Users with Remote Access shall protect that access from abuse and compromise.
2. Users with Remote Access privileges are responsible for ensuring that their use of this service complies with this and all other University policies and regulations. Users shall limit their Remote Access session to their own use. Users may not alter the configuration of the Remote Access connection to University Information Resources, Information Systems, or Electronic Resources.

I. Network Security

IT managers and IT Technicians shall control and protect access to both internal and external network services.

1. University Information Technology (UIT) has the operational responsibility for managing the University's network.
2. UIT shall:

   a. establish appropriate Controls and segmentation between internal University networks, external University networks, networks owned by other organizations, and public networks (wired and wireless) to protect the confidentiality, integrity, and availability of Information Assets;

   b. establish appropriate authentication and access Control mechanisms for Users, IT Resources, and Information Systems; and

c. periodically monitor implementation of Controls to ensure consistency across the University's network infrastructure.

J. Log Management and Monitoring

1. IT Technicians shall configure IT Resources, Information Systems, and Electronic Resources to record and monitor IT Security Incidents, events, and weaknesses. IT Technicians shall review and analyze Logs for indications of inappropriate or unusual activity.

2. IT Technicians shall protect Logs from tampering, shall limit access to Logs, and are accountable for the integrity of Logs for the Information Systems, IT Resources, and Electronic Resources they are responsible for.

For more specific implementation requirements, please access Rule R4-004J.

K. Backup and Recovery

1. To ensure that University Information Assets are available in the event of a disruption, error, or disaster, IT managers and IT Technicians shall implement the following Controls for the systems for which they are responsible:

a. backups shall be Encrypted;

b. backups containing Information Assets subject to local, state, federal laws and regulations, or contractual obligations shall be maintained in accordance with those requirements;

c. backups shall be protected; and

d. backups shall be tested for integrity.

L. Information System Media Handling

1. IT managers and IT Technicians shall inventory, control, and physically protect Information System Media for which they are responsible. Information System Media shall be Encrypted to prevent Unauthorized Access, disclosure, modification, removal, or destruction of Information Assets and

interruption to the University's business activities. IT Technicians shall implement the associated procedures to protect Information System Media, from Unauthorized Access, disclosure, modification, removal, and destruction.

a. Media Access: IT Technicians shall restrict access to Information System Media to authorized individuals.

b. Media Storage: IT Technicians shall physically control and securely store Information System Media on-site within controlled areas. IT managers shall ensure any authorized off-site storage is secured at the same level or higher.

c. Media Transport: IT Technicians shall protect, control, and maintain a detailed record of Information System Media transported outside of controlled areas and restrict the activities associated with the transport of such media to authorized personnel.

d. Media Sanitization and Disposal: IT Technicians shall sanitize or destroy Information System Media containing Restricted or Sensitive Data prior to disposal or release for reuse.

M. Business Continuity and Disaster Recovery Planning

1. The University administration, executive UIT/ITS leadership, and IT managers shall develop, review, test, and update a formal, documented business continuity and disaster recovery plan which incorporates University policy and contractual and regulatory requirements.

N. IT Security Incident Management

1. The University shall develop and periodically review, test, and update a formal, documented IT Security Incident response plan that addresses purpose, scope, roles, responsibilities, management commitment, coordination among University administrative units and entities, escalation procedures, and compliance. The University shall develop and periodically

review and update a formal, documented procedure to facilitate the implementation of the IT Security Incident response plan. All University Users shall report any observed or suspected IT Security Incidents upon discovery as quickly as possible to their respective help desk.

O. IT Security Awareness and Training

1. The IT security awareness and training program is designed to educate Users to recognize key IT security concerns and respond accordingly.

   a. All Users shall participate in IT security training at least annually.

   b. The Information Security Office shall review the IT security awareness and training program at least quarterly to ensure the training is current and addresses relevant topics. The Chief Information Security Officer shall approve the training.

   c. The Information Security Office shall record security training participation and completion.

   d. The Chief Information Security Officer shall establish additional training requirements for personnel with system administration and IT security roles and responsibilities.

P. Exceptions to Policy

1. Exceptions to this policy and any related rules or procedures may be requested through the Information Security Office's Governance, Risk, and Compliance team if the cost to remediate systems and processes greatly exceeds the Risks of noncompliance.

2. Only the Chief Information Security Officer, the Chief Technology Officer, and the cognizant vice president, dean, or other person in a position of similar seniority able to accept Risk on behalf of the University may approve an exception to this policy or related regulations.

3. Please contact the ISO-GRC team for details and assistance with the exception process.

Q. Violations

1. All Users shall report incidences of actual or suspected noncompliance with this policy or associated regulations to the Information Security Office, whose administrators shall work with the appropriate authorities to resolve.
2. The University reserves the right to revoke access to any resource for any User who violates this policy or associated regulations, or for any other business reasons in conformance with applicable policies.
3. Violation of this policy or associated regulations shall result in disciplinary action in accordance with pertinent University policies, and as outlined in Rule R4-004Q: Information Security Policy Sanctions.

For more specific implementation requirements, please access Rule R4-004Q.

Sections V- VIII are for user information and are not subject to the approval of the Academic Senate or the Board of Trustees. The Institutional Policy Committee, the Policy Owner, or the Policy Officer may update these sections at any time.

V. Policies/Rules, Procedures, Guidelines, Forms, and Other Related Resources

A. Rules.

1. Rule R4-004A: Acceptable Use
2. Rule R4-004C: Data Classification and Encryption
3. Rule R4-004D: Access Management
4. Rule R4-004F: Physical and Facility Security
5. Rule R4-004G: IT Resource and Information System Security and Vulnerability Management

6. Rule R4-004J: Log Management and Monitoring
7. Rule R4-004Q: Information Security Policy Sanction Matrix

B. Procedures, Guidelines, and Forms.

1. Procedure P4-004E: Change Management
2. Procedure P4-004G: Vulnerability Management
3. Procedure P4-004G1: Configuration Hardening
4. Procedure P4-004I: Network Security
5. Procedure P4-004J: Log Management and Monitoring
6. Procedure P4-004K: Backup and Recovery
7. Procedure P4-004L: Media Handling
8. Procedure P4-004M: Business Continuity and Disaster Recovery Planning
9. Procedure P4-004N: IT Security Incident Management
10. Procedure P4-004P: Exceptions to Policy

C. Other Related Resources. [*reserved*]

VI. References

A. 45 C.F.R. 164: Health Insurance Portability and Accountability Act (HIPAA): Security and Privacy

B. Family Educational Rights and Privacy Act of 1974 (“FERPA”, 20 U.S.C. § 1232g)

C. Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541)

D. ISO 27002:2013, Information Technology - Security Techniques - Code of Practice for Information Security Management

E. NIST 800 Series, Federal Information Security Standards

F. Policy 3-070: Payment Card Acceptance

G. Policy 4-001: University Institutional Data Management

H. Policy 4-003: World Wide Web Resources Policy

I. Policy 5-111: Disciplinary Actions and Dismissal of Staff Employees

J. Policy 6-400: Code of Student Rights and Responsibilities

K. Policy 6-316: Code of Faculty Rights and Responsibilities

L. Pub. 111-5, Division A, Title XIII, Subtitle D: Health Information Technology for Economic and Clinical Health Act (HITECH Act)

M. Omnibus HIPAA Rule: 45 CFR Parts 160 and 164 - Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule

N. Utah Board of Higher Education Policy R345: Information Technology Resource Security

VII. Contacts

The designated contact officials for this Regulation are:

A. Policy Owner(s) (primary contact person for questions and advice): Chief Information Security Officer

B. Policy Officer(s): Chief Information Officer

See Rule 1-001 for information about the roles and authority of policy owners and policy officers.

VIII. History

Revision History

A. Current version. Revision 5.

1. Approved as an Interim Policy by President Randall on September 12, 2023 with effective date of September 12, 2023. Approved with no changes by the Board of Trustees on November 14, 2023.
2. Legislative History
3. Editorial Revisions

B. Previous versions.

1. Revision 4. Effective date May 12, 2015.
2. Revision 3. Effective date December 13, 2011.
3. Revision 2. Effective date September 23, 2009.

C. Renumbering

1. Renumbered from PPM 1-18.