Policy 4-004: University of Utah Information Security Policy

I. Purpose & Scope

A. The purpose of the University Information Security Policy is to:

1. Maintain the confidentiality, integrity, and availability of all systems supporting the mission and functions of the University of Utah.
2. . Ensure compliance with all applicable federal, state, and local laws, regulations and statutes, as well as contractual obligations.
3. Ensure the protection of the University's Information Technology (“IT”) resources from unauthorized access or damage.

B. Compliance with this Policy, and all its related Rules and Procedures, is required for all of the University's 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, vendors, and third party agents.

II. Definitions

A. Account - A login ID in combination with a password or other authentication token used to access any of the University's IT resources.

B. Assessed Level of Risk - Risk as assessed by the Information Security and Privacy Office or by using a methodology approved by that office (including self-assessments).

C. Availability - Ability of an IT service to perform its function when required.

D. Chief Information Officer (CIO) - The Chief Information Officer is responsible for the University's IT planning, budgeting, and performance including its information security components. Decisions made in these areas shall be based on an effective information security program.

E. Chief Information Security and Privacy Officer (CISPO) - The Chief Information Security Officer is responsible for the development and maintenance of security strategy for the University's IT resources and oversight of information security incidents.

F. Confidential - Any data which is classified as "restricted" or "sensitive" per the data classification model.

G. Confidentiality - A security principle that requires that data should only be accessed by authorized personnel.

H. Data Steward - As defined in Policy 4-001, the University Data Management. {link}

I. Information Security and Privacy Office (ISPO) - The Information Security and Privacy Office is responsible for the development and maintenance of security strategy for the University's IT resource systems, risk assessments, compliance with regulations, policies, rules and procedures, and for the oversight of information security incidents. It plays a leading role in ensuring informed decisions about risk are made by the appropriate individuals within the University, and overall accountability for those decisions are understood and documented. Together, with data stewards and governance groups, the ISPO defines controls and standards to achieve policy objectives.

J. Information Security Operations (ISO) - Information Security Operations is responsible for the day-to-day implementation of operational and tactical IT security tools and methodologies to achieve the University's strategic security goals.

K. IT Resource - A workstation (PC, Mac, etc.), server, smartphone, biomedical device, networking device, web camera (cameras or other monitoring devices), or other device/resource that is a) owned by the University; b) device used to conduct University business regardless of ownership; c) that is connected to the University's network; and/or d) that is accessing, maintaining, or transmitting University data and used for electronic storage, processing or transmitting of any data or information.

L. IT Resource Media - Physical media that contains the University's data. This definition includes but is not limited to hard drives, backup tapes, CD-ROM, DVD-ROM, Blu-Ray, USB drives, recorded magnetic media, photographs, digitized information or microfilm.

M. Integrity - A security principle that ensures data is only modified by authorized personnel and activities. Integrity considers all possible causes of modification, including software and hardware failure, environmental events, and human intervention.

N. IT Resource Administrator - The individual who has day-to-day operational responsibility for an IT resource.

O. Remote Access - The process of accessing the University's information or IT resources from IT resources that are not managed by the

University.

P. Risk - A function of the likelihood of a given threat-source exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization.

Q. Server - Hardware or software used to provide information and/or services to multiple users.

R. System - A functionally related group of software, hardware and IT resources.

S. Unauthorized Access - Access to any IT Resource, without the permission of the appropriate steward/owner.

T. The University of Utah ("University") - includes all administrative units, including colleges, divisions, departments, and centers, and all members of the University community, including students, staff, faculty, and other permanent and temporary employees.

U. User - Any person, including students, staff, faculty, permanent and temporary employees, contractors, vendors, automated processes (acting as a user), and third party agents, who accesses any University IT resources.

V. Workstation - An electronic computing device, for example a laptop or desktop computer, or any other device that performs similar functions (i.e. smartphone, handheld device), and electronic media stored in its immediate environment.

III. Policy

A. Users have the responsibility to ensure the protection of the University's information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction by complying with the information security requirements maintained in this Policy.

B. Roles and Responsibilities

1. Information Security Liaisons

   a. Appointments of Information Security Liaisons shall be made by the Vice President who is responsible for the Information Security Liaison's functional area. Multiple Information Security Liaisons may be appointed to accommodate the size and scope of the functional area. These appointees will act as the central point of coordination for security and privacy related activities.

2. Information Security and Privacy Advisory Committee

   a. The Information Technology Council (see Policy 4-001) has the authority to establish an Information Security and Privacy Advisory Committee. The Advisory Committee's primary charge shall be to evaluate the impact of information security policies and practices on staff, faculty, students, employees, and others who utilize services at the University.

C. Risk Assessment

1. The University must regularly identify, define and prioritize risks to the confidentiality, integrity, and availability of their IT Resources utilizing a methodology approved by the Information Security and Privacy Office (ISPO). The ISPO will provide guidance or assistance for the risk assessment process as necessary.

2. In addition to regular risk assessments, the University must conduct a risk analysis, in consultation with ISPO, when environmental or operational changes or additions occur (new services, systems, etc.) which significantly impact the confidentiality, integrity or availability of information systems containing confidential information.

D. Data Management

1. The University shall take measures to protect confidential information that is stored, processed or transmitted using IT resources. These measures shall be implemented commensurate with the assessed level of risk and reviewed at regular intervals.

2. The storage of data classified as restricted is not permitted, unless:

   a. The User requires such restricted information to perform duties that are necessary to conduct the business of the University;

   b. The cognizant Data Steward grants, in writing, permission to the user; AND

   c. The User and all IT resources storing the restricted data fully comply with this Policy and associated Regulations and may be subject to an assessment prior to approval.

3. Data Classification - All electronic data shall be classified in accordance with the following requirements:

a. PUBLIC DATA is information that may or must be open to the general public. It is defined as information with no existing local, national or international legal restrictions on access or usage. Public data, while subject to University disclosure rules, is available to all members of the University community and to all individuals and entities external to the University community. By way of illustration only, some examples of Public Data include:

   i. Campus maps

   ii. Campus events

   iii. Course descriptions

b. SENSITIVE DATA is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a criminal or civil statute requiring this protection. Sensitive Data is information that is restricted to members of the University community who have a legitimate purpose for accessing such data. By way of illustration only, some examples of Sensitive Data include:

   i. Internal memoranda and electronic mail, and non-public reports, budgets, plans, and financial information.

   ii. Library transactions.

   iii. Information covered by non-disclosure agreements

   iv. Donor contact information and non-public gift amounts.

c. RESTRICTED DATA is information protected by federal or state statutes or regulations, University Regulations or contractual language. Restricted Data may be disclosed to individuals on a need-to-know basis only. By way of illustration only, some examples of Restricted Data include:

   i. Credit Card Information

   ii. Protected Health Information

   iii. Social Security numbers

   iv. Student and prospective student information

   v. Export controlled information under U.S. laws

4. Departments should carefully evaluate the appropriate data classification category for their information.

5. Data Handling - All electronic data shall have appropriate handling procedures in accordance with its classification and commensurate with the assessed level of risk.

E. Access Management

1. Only authorized users shall have physical, electronic or other access to the University's IT resources. Access shall be limited to users with a business need to know, and limited only to the requirements of their position at the University. It is the shared responsibility of IT resource administrators and users to prevent unauthorized access to the University's systems. Access controls for IT resources shall include effective procedures for granting authorization, tools and practices to authenticate authorized users, and prevention and detection of unauthorized use. IT Resource Administrators and managers are primarily responsible for establishing, documenting, implementing, and managing access control procedures for their IT resources.

   a. Access Authorization - The University's accounts shall be issued after the request is authorized and documented.

   b. Account Authentication - The University's accounts shall be authenticated at a minimum via unique login IDs and passwords.

   c. Access Termination - The University's accounts shall be disabled and/or deleted immediately after notification of termination of contract, employment, or relationship with the University. [Note 1]

   d. Access Reaccreditation - The University shall conduct periodic reviews of authorized access commensurate with the assessed level of risk.

   e. Emergency Access Procedures - The University shall establish, as appropriate, procedures for obtaining necessary information during an emergency.

F. Change Management

1. Administrative units responsible for information resources will ensure that they have and follow approved change management procedures that include a security review.
2. Whenever possible, changes that impact users and other IT Resource Administrators will be communicated prior to the change.

G. Physical and Environmental Security

1. The University shall physically protect IT Resources commensurate with the assessed level of risk. Users and IT Resource Administrators shall ensure that controls are planned and implemented for safeguarding physical components against compromise and environmental hazards. Locks, cameras, alarms, redundant power systems, fire detection and suppression systems, and other safeguards as appropriate shall be installed in data centers and technology closets to discourage and respond to unauthorized access to electronic or physical components contained in these areas.
2. Administrative units in which activities covered by the Health Insurance Portability and Accountability Act ("HIPAA") occur must develop procedures to document repairs and modifications to the physical security components of a facility.

H. IT Resource Security

1. The University shall protect IT Resources commensurate with the assessed level of risk and utilize security baseline settings to ensure that IT resources are available for use and free from malware. IT Resource Administrators and users managing IT resources shall:
    a. Protect any IT resource under their management from compromise. This includes installing antivirus and relevant security patches to address security issues.
    b. Implement procedures that terminate an electronic session after a predetermined time of inactivity.
    c. Configure the IT resources to reduce vulnerabilities to a minimum.
    d. Periodically verify audit and activity logs, examine performance data, and generally check for any evidence of unauthorized access, the presence of viruses or other malicious code.
    e. Cooperate with ISPO and ISO by providing support for and/or review of administrative activities as well as allowing the performance of more sophisticated procedures such as penetration testing and real-time intrusion detection.

I. Remote Access

1. Users who use an IT resource to create, access, transmit or receive University of Utah information are responsible for protecting that information in a manner commensurate with risk. Appropriate procedures regarding confidentiality and privacy of information should be followed at all times regardless of location on or off-campus.
2. IT resources that contain restricted data will be available for remote access upon the data steward's approval.
3. The cognizant data steward must outline the requirements for remote access to, or use of, protected health information.

J. Vendors and Business Services Agreement

1. . The University may permit a vendor, or other third party, to create, receive, maintain, or transmit confidential University information when satisfactory assurances are obtained that the vendor will appropriately safeguard the information.

K. Network Security

1. Access to both internal and external networked services shall be controlled, restricted, and protected by IT resource administrators, commensurate with the assessed level of risk. The University's user and/or IT resource access to networks and network services shall not compromise the security of the network services. This shall be accomplished by ensuring:
    a. Appropriate controls are in place between the University's network and networks owned by other organizations, and public networks.
    b. Appropriate authentication mechanisms are applied for users and IT resources.
    c. Control of user and IT resource access to information services is enforced.

L. Log Management and Monitoring

1. IT Resource Administrators shall configure IT Resources to record and monitor information security incidents, events and weaknesses. IT resource administrators shall regularly review and analyze these logs for indications of inappropriate or unusual activity.
2. For more information about individual privacy protection requirements, see Policy 4-002-V-B: Information Resources Policy, Privacy.

M. . Backup and Recovery

1. IT resource administrators shall conduct backups of user-level, application-level, and system-level information commensurate with the assessed level of risk and protect backup information at the storage location. Routine procedures shall be established for taking backup copies of data and testing their timely restoration and recoverability.
2. Measures to protect backup media shall be commensurate with the importance and sensitive of the data.
3. Measures may include physically secured, encrypted, off-site copies (See Data Management - Data Handling).

N. IT Resource Media Handling

1. The University's IT resource media shall be controlled and physically protected by users, commensurate with the assessed level of risk to prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities. Appropriate operating procedures shall be established to protect documents, IT resource media, input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction.
    a. IT Resource Media Access - The University shall restrict access to IT resource media to authorized individuals.
    b. IT Resource Media Storage - The University shall physically control and securely store IT resource media on-site within controlled areas where appropriate, and ensure any authorized off-site storage is, at minimum, secured at the same level as the on-site area.
    c. IT Resource Media Transport - The University shall label IT resource media prior to transport, protect and control IT resource media during transport outside of controlled areas, and restrict the activities associated with transport of such media to authorized personnel.
    d. IT Resource Media Sanitization and Disposal - The University shall appropriately sanitize or destroy IT resource media prior to disposal or release for reuse.

O. Business Continuity and Disaster Recovery Planning

1. The University shall develop and periodically review, test and update a formal, documented, contingency plan based on a business impact analysis that addresses purpose, scope, roles, responsibilities, management commitment, coordination among University administrative units and entities, escalation procedures and compliance, as well as develop and periodically review, test and update formal, documented procedures to facilitate the implementation of the contingency plan.
2. Where appropriate, the University must develop contingency plans that allow physical access to facilities in order to recover data and resume operations in the event of an emergency or disaster (for example, if card access to the data center were to fail).
3. As needed, the University shall establish (and implement as necessary) procedures to enable continuation of critical business processes for protection of the security of information while operating in emergency mode.

P. Information Security Incident Management

1. The University shall develop and periodically review, test and update a formal, documented, incident response plan that addresses purpose, scope, roles, responsibilities, management commitment, coordination among University administrative units and entities, escalation procedures and compliance, as well as develop and periodically review and update a formal, documented procedure to facilitate the implementation of the incident response plan. All students, faculty, staff, permanent and temporary employees, contractors and third party agents shall be made aware of the procedures for reporting incidents, events and weaknesses that may have an impact on the security of University IT resources and any associated data, and they shall be required to report these incidents, events and weaknesses to the appropriate point of contact as soon as possible.
2. The University may discontinue service to any User who violates this policy or other IT policies when continuation of such service

threatens the security (including confidentiality, integrity, and availability) of the University's IT Resources. The University may discontinue service to any network segment or networked device if the continued operation of such segments or devices threatens the security of the University's IT Resources. The User's access shall be restored as soon as the direct and imminent security threat has been remedied.

Q. Information Security Awareness and Training

1. The University's students, faculty, staff, permanent and temporary employees and, where appropriate, contractors and third party users shall receive information security awareness training and regular updates on the University's policies, rules and procedures, as relevant for their role at the University.
    a. Information Security Awareness - The University shall provide basic security awareness training to all IT resource system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and periodically thereafter.
    b. Information Security Training - The University shall identify personnel that have significant IT resource system information security roles and responsibilities, documents those roles and responsibilities, and provides appropriate information system security training before authorizing access to the system or performing assigned duties, when required by system changes; and periodically thereafter.
    c. Information Security Training Records - The University shall document and monitor individual IT resource system information security training activities including basic security awareness training and specific information system security training.
    d. Contacts with Security Groups and Associations - The University shall establish and maintain contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of information security professionals in similar organizations to stay up to date with the latest recommended information security practices, techniques, and technologies and to share the latest information security related information including threats, vulnerabilities, and incidents.

R. Exceptions to Policy

1. Exceptions to this Policy and any related Rules or Procedures may be made where the cost to remediate systems and processes that are not compliant with applicable University Regulations greatly exceeds the risks of non-compliance.
2. Exceptions to this Policy received and approved by ISPO and Data Stewards will be documented and archived.
3. Exception requests are reviewed and analyzed by ISPO and the Data Steward (or designee), and if the request creates significant risks without compensating controls it may not be approved. If denied, appeals may be made to the Chief Information Officer.
4. Exceptions may be requested via: http://www.secureit.utah.edu/ispo/exceptions.html

S. Violations

1. Incidences of actual or suspected non-compliance with this Policy or associated Regulations must be reported to the Information Security and Privacy Office, whose administrators will work with the appropriate authorities to resolve.
2. The University reserves the right to revoke access to any Information Technology 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 may result in disciplinary action in accordance with pertinent University policies, including those referenced in Section V of this policy.

[Note: Parts IV-VII of this Regulation (and all other University Regulations) are Regulations Resource Information – the contents of which are not approved by the Academic Senate or Board of Trustees, and are to be updated from time to time as determined appropriate by the cognizant Policy Officer and the Institutional Policy Committee, as per Policy 1-001 and Rule 1-001.]

IV. Rules, Procedures, Guidelines, Forms and other related resources

A. Rules

Rule 4-004A (/it/rules/Rule4-004A-2.pdf): Protected Health Information Data Breach Notification Procedures

Rule 4-004B (/it/rules/Rule4-004B.php): Information Security and Privacy Training and Awareness

Rule 4-004C (/it/rules/Rule4-004C.php): Information Security Incident Response Rule

Interim Rule 4-004D (/it/rules/Rule4-004D.php): Health Sciences Encryption of Protected Health Information

B. Guidelines

G4-004B (/it/guidelines/G4-004B.pdf): Information Security and Privacy Liaisons

G4-004D (/it/guidelines/G4-004D.pdf): Cloud Computing: Opportunities Used Safely

G4-004E (/it/guidelines/G4-004E.pdf): Termination Check List for Information Technology

G4-004H1 (/it/guidelines/G4-004H1.pdf): Portable Device Security

G4-004H3 (/it/guidelines/G4-004H3.pdf): IT Resource Security: Vulnerability Management

G4004J (/it/guidelines/G4-004J.pdf): Vendors and Business Services Agreements

G4-004L (/it/guidelines/G4-004L.pdf): Log Management and Monitoring

G4-004N1 (/it/guidelines/G4-004N1.pdf): Media Sanitization and Destruction

G4-004Q (/it/guidelines/G4-004Q.pdf): Privacy and Information Security Training and Awareness Contacts

G4-004S (/it/guidelines/G4-004S.pdf): Sanctions Matrix Guidelines

C. Forms (Reserved)

D. Other related source materials

V. 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 27002:2005, Information Technology - Security Techniques - Code of Practice for Information Security Management

E. NIST 800 Series (http://csrc.nist.gov/publications/PubsSPs.html), Federal Information Security Standards

F. Policy 3-070 (/administration/3-070.php): Payment Card Acceptance

G. Policy 4-001 (/it/4-001.php): University Institutional Data Management

H. Policy 4-002 (/it/4-002.php): Information Resources Policy

I. Policy 4-003 (/it/4-003.php): World Wide Web Resources Policy

J. Policy 5-111 (/human-resources/5-111.php): Disciplinary Actions and Dismissal of Staff Employees

K. Policy 6-400 (/academics/6-400.php): Code of Student Rights and Responsibilities

L. Policy 6-316 (/academics/6-316.php): Code of Faculty Rights and Responsibilities

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

N. Utah System of Higher Education Policies and Procedures (http://higheredutah.org/sbr/policy/policies.htm)

VI. Contacts:

The designated contact officials for this Policy are:

A. Policy Owner (primary contact person for questions and advice): Chief Information Security and Privacy Officer, 801-587-9241 IT_policy@utah.edu

B. Policy Officer: Chief Information Officer, 801-581-3100

These officials are designated by the University President or delegee, with assistance of the Institutional Policy Committee, to have the following roles and authority, as provided in University Rule 1-001:

"A 'Policy Officer' will be assigned by the President for each University Policy, and will typically be someone at the executive level of the University (i.e., the President and his/her Cabinet Officers). The assigned Policy Officer is authorized to allow exceptions to the Policy in appropriate cases.... "

"The Policy Officer will identify an 'Owner' for each Policy. The Policy Owner is an expert on the Policy topic who may respond to questions about, and provide interpretation of the Policy; and will typically be someone reporting to an executive level position (as defined above), but may be any other person to whom the President or a Vice President has delegated such authority for a specified area of University operations. The Owner has primary responsibility for maintaining the relevant portions of the Regulations Library... .[and] bears the responsibility for determining -requirements of particular Policies... ." University Rule 1-001-III-B & E

VII. History

Renumbering: Renumbered as Policy 4-004 effective 9/15/08, formerly known as PPM 1-18

A. Current version: Revision 3, effective date: December 13, 2011

Approved by Academic Senate: December 5, 2011

Approved by Board of Trustees: December 13, 2011

Background information (/it/appendices_4/Background_4-004_12-2011.pdf) for this version

B. Earlier revisions:

Revision 2 (/it/revisions_4/4-004.R2.pdf): effective dates - September 23, 2009 to December 12, 2011

---

1. This provision is intended to ensure that access is removed for persons lacking an appropriate relationship with the University. The Policy allows for flexibility by administrators of Human Resouces, Student Affairs, and other administrative units to define the appropriate relationships (e.g., staff, faculty person of interest, alumni, etc.)