Policy 4-004: University of Utah Information Security Policy. Rev 4

I. Purpose and Scope

A. 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. 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, research collaborators, vendors, and third party agents.

II. Definitions

For the purposes of this Policy and any associated Regulations, these words and phrases have the following meanings:

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

B. **Account Provisioners** - IT personnel responsible for the creation, managment 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 is used to provide a specific service to a community of users, or is used 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. **Audit Log** - A chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.

F. **Audit Trail** - A record showing who has accessed an Information System and what operations the User has performed during a given period of time.

G. **Automated Monitoring** - Service or function of an autonomous monitoring tool that correlates and analyzes audit logs and alerts across multiple security technologies.

H. **Change** - An event or action which modifies the configuration of any component, Application, Information System, or Service.

I. **Confidential** - Any Information Asset which is classified as Restricted or Sensitive per the Data Classification and Encryption Rule

J. **Control** - A control is a means of managing risk, including policies, rules, procedures, processes, practices or organizational structures, which can be of administrative, technical, physical, management, or legal nature. Control is also used as a synonym for safeguard or countermeasure.

K. **Critical Workstations** - Workstations running time-sensitive Applications. These include, but are not limited to, Workstations in Lab, Pharmacy, Radiology and Emergency Downtime departments throughout the University's hospitals and clinics.

L. **Dual-homing** - A term used to reference a fault-tolerant scheme that uses more than one network interface.

M. **Electronic Resource** - Any resource used for electronic communication, including but not limited to internet, Email, and social media.

N. **Email** - A means for exchanging digital messages between two parties sent via any electronic means.

O. **Encryption** - To alter information using a code or mathematical algorithm so as to be unintelligible to unauthorized readers.

P. **Event Logs** - A log service which reports on specified events such as a failure to start a component or complete an action. The three common Information System Event Log sources are Application, Security, and System.

Q. **FIPS** - Federal Information Processing Standard

R. **Firewall** - A device or program that controls network traffic flow between networks or hosts that employ disparate security policies.

S. **HHS** - Health and Human Services

T. **HIPAA** - Health Information Portability and Accountability Act

U. **Illegal Behavior** - Any activity that is prohibited by local, state, or federal law or regulation.

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

W. **Information Security Incidents** - Events or weaknesses that jeopardize the confidentiality, integrity, and availability of the University's Information Assets, IT Resources, and Information Systems.

X. **Information System** - An Application or group of Servers used for the electronic storage, processing, or transmitting of any University data or Information Asset.

Y. **Information System Media** -Physical media on which an Information System's Information Assets are stored for backup and recovery purposes (e.g. backup tapes, backup disks, NAS/SAN drives, magnetic media, etc.).

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

AA. **IS** – Information Security

BB. **IT** – Information Technology

CC. **IT Technicians** – IT Technicians develop, administer, manage and monitor the IT Resources, Information Systems, and Electronic Resources that support the University's IT infrastructure, are responsible for the security of the IT Resources, Information Systems, and Electronic Resources they manage, and assure that security-related activities are well documented and completed in a consistent and auditable manner.

DD. **IT Resource** – A Server, Workstation, Mobile Device, medical device, networking device, web camera or other monitoring device, or other device/resource that is a) owned by the University or used to conduct University business regardless of ownership; b) connected to the University's network; and/or c) that is creating, accessing, maintaining, or transmitting Information Assets and used for electronic storage, processing or transmitting of any data or information.

EE. **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, Windows tablet, etc.).

FF. **Mobile Code** – Software transferred between IT Resources and executed on a local system without explicit installation or execution by the recipient. Examples include, but are not limited to, scripts such as JavaScript or VBScript, Java applets, ActiveX controls, Flash, and macros embedded in Microsoft Office documents.

GG. **NIST** – National Institute of Standards and Technology

HH. **Patch** – A fix to a program failure, bug, or vulnerability that may also be referred to as a Service Pack.

II. **PHI** – Protected Health Information

JJ. **PII** – Personally Identifiable Information

KK. **Reasonable Suspicion** – A legal term used to describe a set of circumstances that indicate the basis for taking some action in connection with an individual. In order to qualify as "reasonable", the suspicion must be tied to a particular employee rather than a group of employees, and the suspicion must be based on specific and articulable facts, along with rational inferences taken from those facts.

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

MM. **Removable Media** - Physical media that is attached to or easily removed from a Workstation or Mobile Device, on which the Workstation's or Mobile Device's Information Assets are stored for backup and sharing purposes (e.g. USB drives, thumb drives, external hard drives, DVDs, CDs, etc.).

NN. **Restricted Data** – Any data types classified as Restricted per the Data Classification and Encryption Rule.

OO. **Risk** - Risk is 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)

Inherent Risk – Inherent Risk is defined as the likelihood and impact of loss arising out of circumstances or existing in an environment, IT Resource, or Information System in the absence of any action to control or modify the circumstances.

Residual Risk – Residual Risk is the risk of an IT Resource that remains after controls or other mitigating factors have been implemented.

PP. **Sensitive Data** – Any data type classified as Sensitive per the Data Classification and Encryption Rule.

QQ. **Server** – Hardware and software, and/or Workstation used to provide information and/or services to multiple Users.

RR. **Service Account** – An Account created specifically for running a process for an Application, Information System, or software package.

SS. **Signature-based Detection** – Identifying potential incidents by matching each input event against defined patterns that model malicious activity, and executing actions based on rules defined in the detection system. Signature-based detection systems are tuned to identify attacks with a level of accuracy that reduces the occurrence of false positive results.

TT. **Split-tunneling** – A computer networking concept which allows a mobile user to access dissimilar security domains like a public network (e.g., the Internet) and a local area network or wide area network at the same time, using the same or different network connections.

UU. **Threat** - A threat is anything (natural, facility, and/or human) that has the potential to cause harm.

VV. **Unauthorized Access** - Obtaining access 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.

WW. **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.

XX. **VPN** – A Virtual Private Network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to the University's network.

YY. **Vulnerability** - A weakness that could be used to endanger or cause harm to an Asset.

ZZ. **Workstation** - An electronic computing device, terminal, or any other device that performs as a general-purpose computer equipped with a microprocessor and designed to run commercial software (such as a word processing application or Internet browser) for an individual User (e.g. laptop, desktop computer, PC, Mac, etc.).

III. 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. Personal use of IT Resources, Information Systems, and Electronic Resources may be authorized if the use does not interfere with University duties, and does not violate the terms of any University regulation.

1. IT Resource and Information System Use

All Users of University IT Resources and Information Systems shall:

a. Comply with all federal, state and other applicable laws, all generally applicable University regulations, and all applicable contracts and licenses. Users are responsible for ascertaining, understanding, and complying with the laws, policies, rules, procedures, contracts, and licenses applicable to their particular uses.

b. Use only those University IT Resources and Information Systems that they are authorized to use and use them only in the manner and to the extent authorized.

c. Refrain from unauthorized attempts to circumvent the security mechanisms of any University IT Resource or Information System.

d. Refrain from attempts to degrade system performance or capability.

e. Refrain from attempts to damage IT Resources, Information Systems, software, or Intellectual Property of others.

2. Account Use

All Users of University Accounts shall:

a. Refrain from sharing an Account and/or password or any other authentication token, or using another User's Account and/or password or any other authentication token. All such activity is strictly prohibited.

b. Refrain from unauthorized viewing or use of another User's Accounts, computer files, programs, and/or data. Access to such information does not imply permission to view or use it. All such activity is strictly prohibited.

3. Electronic Resource Use

All Users of Electronic Resources shall:

a. Utilize Electronic Resources for purposes consistent with the University's values, policies, and its applicable information security rules and procedures.

b. Protect the access to and integrity of Electronic Resources.

c. Abide by local, state, federal or applicable international laws, contractual obligations, regulations, the University's regulations, and respect the copyrights and Intellectual Property rights of others.

d. Use Electronic Resources only for their intended purpose.

e. Respect the privacy and personal rights of others.

4. Intellectual Property Use

All Users of Intellectual Property shall:

a. Refrain from the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the University.

b. Abide by federal copyright laws when using University IT Resources and Information Systems for the use of or the 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.

c. Refrain from violating the rights of any person or company protected by trade secret, patent, or any other intellectual property, or similar laws or regulations.

For more specific implementation requirements, please see the Acceptable Use Rule.

B. Information Security Risk Management

The University's Information Security Risk Management Program shall support the University's business missions while also mitigating financial, operational, reputational and regulatory compliance risk. Risk Management shall enable the University to accomplish its mission(s) by:

1. Securing the Information Systems that create, maintain, process, or transmit the University's Information Assets

2. Enabling the appropriate University personnel to make well-informed decisions regarding risk and risk management

3. Collaborating with other University risk management activities to ensure the University's information security program priorities are aligned appropriately with the University's risk tolerance

4. Providing a systematic methodology to assess and manage information security risk for the University

For more specific implementation requirements, please see the Information Security Risk Management Rule.

C. Data Classification and Encryption

The University shall take measures to protect Confidential Information Assets that are created, maintained, processed, or transmitted using IT Resources and Information Systems. These measures shall be implemented commensurate with the assessed level of risk and reviewed at regular intervals. IT Technicians are primarily responsible for establishing, documenting, implementing, and managing data handling and management procedures for the IT Resources and Information Systems they support.

1. Data Classification – All Information Assets shall be classified in accordance with the Data Classification and Encryption Rule.

2. Data Handling – All Information Assets shall have appropriate handling Procedures in accordance with the data classification.

3. Encryption – All Information Assets shall have encryption requirements in accordance with data classification.

For more specific implementation requirements, please see the Data Classification and Encryption Rule.

D. Access Management

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 limited only to the requirements of their job function. It is the shared responsibility of IT Technicians and Users to prevent unauthorized access to IT Resources, Information Systems, Information Assets, and Electronic Resources at the University. Access controls shall include effective procedures for granting authorization, tools and practices to authenticate authorized Users, and prevention and detection of unauthorized use.

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

2. Account Authentication – University Accounts shall be authenticated at a minimum via unique login ids and complex passwords.

3. Account Termination – University Accounts shall be deactivated, disabled and/or deleted as soon as reasonably possible after authorized notification of termination of contract, employment, or relationship with the University.

4. Account Reaccreditation – University shall conduct periodic reviews of authorized access commensurate with the assessed level of risk.

For more specific implementation requirements, please see the Access Management Rule.

E. Change Management

Any changes to University production IT Resources and Information Systems that store, process, transmit, or maintain Confidential data shall be authorized, tested, documented, and approved prior to implementation.

For more specific implementation requirements, please see the Change Management Rule.

F. Physical and Facility Security

University IT Resources and Information Systems shall be physically protected commensurate with the assessed level of risk. IT Technicians and IT Personnel 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 ensure protection from natural and facility threats, and to discourage and respond to unauthorized access to electronic or physical components contained in these areas.

For more specific implementation requirements, please see the Physical and Facility Security Rule.

G. IT Resource and Information System Security and Vulnerability Management

IT Resources and Information Systems shall be protected commensurate with the assessed level of risk, and security baseline settings shall be utilized to ensure IT Resources and Information Systems are available for use and guarded against malware.

All IT Technicians, IT Personnel, and Users managing University IT Resources, Information Systems, and Electronic Resources shall:

1. Protect any IT Resources and Information Systems under their management from compromise.

2. Configure the IT Resources and Information Systems to reduce vulnerabilities to a minimum.

3. Install anti-virus and/or other anti-malware tools, and relevant security patches to fix security issues.

4. 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.

5. 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 see the IT Resource/Information System Security and Vulnerability Management Rule.

H. Remote Access

It is the responsibility of Users with remote access privileges to the University's network to ensure that their remote access connection is given, at minimum, the same consideration as the User's on-site connection.

For more specific implementation requirements, please see the Remote Access Rule.

I. Network Security

Access to both internal and external networked services shall be controlled and protected commensurate with the assessed level of risk. User, IT Resource, and

Information System access to networks and network services shall not compromise the security of the network services by ensuring:

1. Appropriate controls are in place between the University's network, networks owned by other organizations, and public networks.

2. Appropriate authentication mechanisms are applied for Users, IT Resources and Information Systems.

For more specific implementation requirements, please see the Network Security Rule.

J. Log Management and Monitoring

University IT Resources, Information Systems, and Electronic Resources shall be configured to record and monitor information security incidents, events and weaknesses. These audit logs shall be regularly reviewed and analyzed for indications of inappropriate or unusual activity.

For more specific implementation requirements, please see the Log Management and Monitoring Rule.

K. Backup and Recovery

The University shall conduct backups of Information Assets commensurate with the Data Classification and Encryption Rule and assessed level of risk, and protect backup information and Information System Media at any storage location. Routine procedures shall be established for taking backup copies of data and testing their timely restoration and recoverability.

For more specific implementation requirements, please see the Backup and Recovery Rule.

L. Information System Media Handling

University Information System Media shall be inventoried, controlled, and physically protected commensurate with Data Classification and Encryption rule with the assessed level of risk to prevent unauthorized disclosure, modification, removal or destruction of Information Assets, and interruption to business activities. Appropriate operating procedures shall be established to protect Information System Media, input/output data, and system documentation from unauthorized disclosure, modification, removal, and destruction.

1. Media Access – The University shall restrict access to Information System Media to authorized individuals.

2. Media Storage – The University shall physically control and securely store Information System 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.

3. Media Transport – The University shall protect and control Information System Media during transport outside of controlled areas, and restrict the activities associated with transport of such media to authorized personnel.

4. Media Sanitization and Disposal – The University shall sanitize or destroy Information System Media containing Confidential data prior to disposal or release for reuse in accordance with NIST guidance.

For more specific implementation requirements, please see the Information System Media Handling Rule.

M. Business Continuity and Disaster Recovery Planning

The University shall develop and periodically review, test and update a formal, documented, business continuity and disaster recovery plan that incorporates information security requirements 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 plans.

For more specific implementation requirements, please see the Business Continuity and Disaster Recovery Planning Rule.

N. Information Security Incident Management

The University shall develop and periodically review, test and update a formal, documented information security 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 information security incident response plan. All Users shall be made aware of the procedures for identifying information security incidents, events and weaknesses that may have an impact on the security of University IT Resources, Information Systems, and Electronic Resources and any associated Information Assets, and the Users shall be required to report these incidents, events and weaknesses to the appropriate point of contact as soon as possible.

For more specific implementation requirements, please see the Information Security Incident Management Rule.

O. Information Security Awareness and Training

All University employees and, where appropriate, other Users shall receive appropriate information security awareness training and regular updates on University regulations, as relevant for their job function.

1. Security Awareness – The University shall provide basic information security awareness to all Users.

2. Security Training – The University shall identify personnel that have significant Information System security roles and responsibilities, document those roles and responsibilities, and provide appropriate Information System security training before authorizing access to the Information System or performing assigned duties, when required by Information System changes, and at least annually thereafter.

3. Security Training Records – The University shall document and monitor individual Information System security training activities including security training, and specific Information System security training.

4. 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 security professionals in similar organizations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents.

For more specific implementation requirements, please see the Information Security Awareness and Training Rule.

P. 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. All approved exceptions to this Policy or any related Rules or Procedures must have an expiration date set no later than one year from the approval date of the exception, and will be reviewed prior to expiration to reevaluate the risks of maintaining the exception based on emerging threats and business justifications.

Q. Violations

1. Incidences of actual or suspected non-compliance with this Policy or associated Regulations must be reported to the Information Security Office, whose administrators will 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 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: Acceptable Use

Rule 4-004B: Information Security Risk Management

Rule 4-004C: Data Classification and Encryption

Rule 4-004D: Access Management

Rule 4-004E: Change Management

Rule 4-004F: Physical and Facility Security

Rule 4-004G: IT Resource and Information System Security and Vulnerability Management

Rule 4-004H: Remote Access

Rule 4-004I: Network Security

Rule 4-004J: Log Management and Monitoring

Rule 4-004K: Backup and Recovery

Rule 4-004L: Information System Media Handling

Rule 4-004M: Business Continuity and Disaster Recovery Planning

Rule 4-004N: Information Security Incident Management

Rule 4-004O: Information Security Awareness and Training

B. Procedures

Policy 4-004 Procedures

C. Guidelines

Guideline: Information Security and Privacy Liaisons

Guideline: Cloud Computing - Opportunities Used Safely

Guideline: Termination Check List for Information Technology

Guideline: Portable Device Security

Guideline: IT Resource Security - Vulnerability Management

Guideline: Vendors and Business Services Agreements

Guideline: Log Management

Guideline: Media Sanitization and Destruction

Guideline: Information Security and Privacy TACs

Guideline: Potential Sanctions for Privacy and Security Violations

D. Forms

E. Other related resource 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 27002:2013, 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

VI. Contacts

The designated contact officials for this Policy are:

A. Policy Owner (primary contact person for questions and advice): Chief Information Security Officer, 801-213-3397

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 4, effective date: May 12, 2015

Approved by Academic Senate: May 4, 2015

Approved by Board of Trustees: May 12, 2015

Approved by Board of Trustees: April 4, 2016

Background information for this version

B. Earlier revisions:

Revision 3: effective dates - December 13, 2011 - May 11, 2015

Revision 2: 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.)