# Rule 4-004A Acceptable Use Rev. 1

## I. Purpose and Scope

A. The purpose of this Acceptable Use Rule is to establish the general parameters for the use of IT Resources, Information Systems and Electronic Resources.

B. This Rule supports section A, titled Acceptable Use, of the University of Utah Information Security Policy 4-004.

## II. Definitions

The definitions provided in Policy 4-004: University of Utah Information Security Policy, apply for purposes of this Rule, including the following:

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

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

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

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

E. **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.

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

G. **IT Resources** - 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.

H. **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.

I. **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.

J. **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.

## III. Rule

The University respects the privacy of employees, faculty, staff, students and other Users of IT Resources, Information Systems and Electronic Resources. Therefore the University does not, absent consent, specifically target an individual User to monitor, review, or access the contents of User email communications, User created

electronic files, or a User's personal device being utilized as an IT Resource, except as set for in this Rule.

The University reserves the right to limit or restrict the use of IT Resources, Information Systems, and Electronic Resources based on business reasons, technical priorities, and financial considerations, as well as when it is presented with reasonable suspicion of a violation of University policies, contractual agreements, or local, state, federal or applicable international laws and regulations.
The University monitors and reviews activities and content on its IT Resources, Information Systems, and Electronic Resources Utilizing Signature-based Detection and Automated Monitoring for the purposes of efficiency, security and operations.

The University further reserves the right to monitor, review and access material stored on, processed, or transmitted through its IT Resources, Information Systems, and Electronic Resources at any time based on reasonable suspicion of Illegal Behavior. The University also reserves the right to access, monitor, and review information on IT Resources, Information Systems, and Electronic Resources for business operations purposes in the case of a User who is unable to perform University duties due to medical illness or emergency, unavailability, or refusal to perform duties.

A. Authorized Use

1. Authorized Users

    a. An authorized User is any individual who has been granted authority by the University to access its IT Resources, Information Systems, Information Assets, and Electronic Resources.

    b. Unauthorized use is strictly prohibited.

    c. If a User ceases being authorized to use University IT Resources, Information Systems, Information Assets, and Electronic Resources, or if such User is assigned a new position and responsibilities, any use for

which that User is not specifically authorized in their new position or circumstances shall cease. A User must not engage in unauthorized use even if the User is mistakenly granted access to or unintentionally permitted to maintain IT Resources, Information Systems, Information Assets, and Electronic Resources.

2. Personal Use

Pursuant to Utah Code Ann. § 78-9-402, when University-owned IT Resources, Information Systems, and Electronic Resources are used or possessed as part of an employee's University duties and the primary purpose of the use or possession by the employee is to fulfill the employee's University duties, this policy authorizes personal use of the IT Resources, information Systems, and Electronic Resources for personal matters.

The University allows Users to make reasonable and limited personal use of its IT Resources, Information Systems, and Electronic Resources to the extent that such use does not interfere with University duties. Individuals using the University's IT Resources, Information Systems, and Electronic Resources for personal business, political campaigning, or other commercial purposes must disclaim a connection between their activities and the University. The University reserves the right to prohibit personal use at any time without prior notice when there is reasonable suspicion of Illegal Behavior or a violation of University regulation has occurred or is occurring.

Authorized Users are responsible for exercising good judgment regarding the reasonableness of personal use, but University management reserves the right to define and approve what constitutes reasonable personal use. Prior use of University Information Systems, Information Assets, and Electronic Resources for personal use does not constitute approval. Personal use of University Information Systems, Information Assets, and Electronic Resources must not interfere with work performance or with the University's ability to use its resources for business purposes. Personal use must not

violate polices, statutes, contractual obligations, or other standards of acceptable behavior. All personal use must be consistent with University regulation.

3. Email Use

   Information that is classified as Restricted should not be sent via Email, regardless of the recipient, without an approved business need and applicable technical controls. The use of encryption is required for Emails containing Restricted data sent to any non-University Email recipient as per the Data Classification and Encryption Rule.

4. Social Media Use

   Users are prohibited from posting on behalf of the University to public newsgroups, websites, blogs, social media or other public media sites without prior management approval. Any social media postings that could reasonably be construed as being on behalf of the University must contain a disclaimer stating that the opinions expressed are strictly the User's own and not necessarily those of University, unless the User is authorized to post on behalf of the University.

5. Cloud Provider Use

   Information that is classified as Restricted should not be stored with a cloud provider unless there is a contractual agreement in place between the University and the cloud service provider that protects the confidentiality of the information and data.

B. Responsible Use

1. Ethical Use

   a. No User may act in ways that violate the Ethical Standards and Codes of Conduct established by the University.

2. Protection of Confidential Information

    a. All Users must maintain the protection of the University's Confidential Information Assets. This requires Users to exercise precautions that include complying with University regulation and taking other precautions to guard Confidential data.

3. Illegal Activities

    a. Under no circumstances are Users authorized to engage in Illegal Behavior while using University IT Resources, Information Systems, Information Assets, and Electronic Resources.

4. Forgery of Communications

    a. Altering electronic communications to hide identity or impersonate another person is considered forgery and is prohibited.

5. Soliciting Business

    a. Users must not use University IT Resources, Information Systems, Information Assets, and Electronic Resources for soliciting business, selling products, or otherwise engaging in commercial activities other than those expressly permitted by University management or other University regulation.

6. Fraud

    a. Users must not use University IT Resources, Information Systems, Information Assets, and Electronic Resources to make fraudulent offers for products, items, or services, or make statements about warranty, expressly or implied.

7. Bandwidth and Overuse

a. Actions detrimental to Electronic Resources, or that negatively affect job performance are not permitted. Excessive use of the University's network bandwidth or other Electronic Resources is not permitted.

b. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance should be performed during times of low University-wide usage.

c. All Users must refrain from acts that waste University Electronic Resources or prevent others from using them.

C. Internet Use

1. Risk of Use

a. Users access the Internet with University facilities at their own risk.

b. The University is not responsible for material viewed, downloaded, or received by Users via the internet. Responsible attitudes and appropriate behavior are essential in using this resource.

c. To protect personal safety and privacy, Internet Users should not give out personal information to others on public resources, without taking into consideration the risks of doing so.

2. Internet Web Browsing

a. Personal use of University systems to access the Internet is permitted during, before, and after business hours, as long as such use follows pertinent policies and guidelines and does not have an adverse effect on the University, its customers, or on the User's job performance.

D. Privacy Expectations

1. Monitoring

a. The University's Information Security Office employees signature-based and automated monitoring activities to ensure compliance with federal, state, and University regulations.

b. The University reserves the right to authorize specific individuals or groups, at times including contracted business partners, to utilize signature-based and automated monitoring activities to monitor IT Resources, Information Systems, and Electronic Resources to ensure compliance with federal, state, and University regulations.

2. Privacy of Stored Personal Information and Electronic Communications

a. University Users have diminished expectations of privacy for any personal information stored on, or sent or received utilizing University-owned IT Resources, Information Systems, and Electronic Resources.

b. Notice to a User will be given when the University accesses a file or electronic communication generated or transmitted by a User, or generated or transmitted by a User's personal device being utilized as an IT Resource. No notice will be given if it is determined by the relevant Data Steward and/or Human Resources, in consultation with University's Office of General that notice will:

i. Unduly impair an investigation of a violation of local, state, federal laws or applicable international laws or regulations;

ii. Seriously hamper the ability of the University to support its missions; or

iii. Result in significant bodily harm or significant property loss or damage.

*[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

TBD

B. Procedures

Policy 4-004 Procedures

C. Guidelines

TBD

D. Forms

E. Other related resource materials

Acceptable Use Frequently Asked Questions

## 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 Controls

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

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

A. Current version: Revision 1, effective date: April 4, 2016

Approved by Academic Senate: May 4, 2015

Approved by Board of Trustees: May 12, 2015

Background information for this version