Rule R4-004A: Acceptable Use

Revision 3. Effective date: September 12, 2023

I. Purpose and Scope 1

II. Definitions 2

III. Rule 3

A. Authorized Use 3

B. Responsible Use 4

C. Internet Use 5

D. Privacy Expectations 5

IV. Policies/ Rules, Procedures, Guidelines, Forms, and other Related Resources 7

V. References 7

VI. Contacts 8

VII. History 8

I. Purpose and Scope

A. Purpose

The purpose of this Acceptable Use Rule is to establish the general parameters for the use of IT Resources, Information Systems, and Electronic Resources. The University respects the privacy of its employees, faculty, staff, students, and other Users of its 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 personal devices used as an IT Resource, except as set forth in this rule.

B. Scope

The scope of this rule 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.

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 apply for this rule. In addition, the terms below apply for the limited purposes of this rule.

A. Automated Monitoring – A service or function of an autonomous monitoring tool that correlates and analyzes Logs and alerts across multiple IT security technologies.

B. Illegal Behavior – Any activity that is prohibited by local, state, or federal law or regulation.

C. Reasonable Suspicion – A legal term used to describe the basis and circumstances for taking some action in connection with an individual. In order to qualify as “reasonable,” the suspicion must be tied to a particular User rather than a group of Users, and the suspicion must be based on specific and articulable facts, along with rational inferences taken from those facts.

D. Signature-based Detection – A method of identifying potential IT Security Incidents by matching each input event against defined patterns that model malicious activity and carrying out actions based on rules defined in the detection system. Signature-based Detection systems are tuned to identify

cyberattacks with a level of accuracy that reduces the occurrence of false positive results.

E. VPN – Virtual private network. A service that uses a public telecommunication infrastructure, such as the internet, to provide remote offices or individual Users with secure access to a different network which may have more cybersecurity requirements.

III. Rule

A. Authorized Use

1. Authorized Users

a. A User may only use a University IT Resource, Information System, Information Asset, or Electronic Resource if the University approves the use. If a User is assigned a new position or responsibilities for which the User no longer needs to use the IT Resource, Information System, Information Asset, or Electronic Resource, the University shall revoke the User's approval and the User shall stop using it. All unauthorized use is strictly prohibited, even if the University mistakenly allows a User access.

b. The University reserves the right to limit or restrict a User's use of IT Resources, Information Systems, Information Asset, and Electronic Resources based on business reasons, technical priorities, or financial considerations, or when presented with Reasonable Suspicion of a violation of University policies; contractual agreements; or local, state, federal, or applicable international laws and regulations.

2. Personal Use

a. 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 shall disclaim a connection between their activities and the University. The University reserves the right to prohibit any User's personal use at any time without prior notice when there is Reasonable Suspicion of Illegal Behavior or a violation of University regulations has occurred or is occurring.

b. The University has no responsibilities to Users for maintaining or providing support for personal use data stored on IT Resources, Information Systems, and Electronic Resources.

c. Users are responsible for exercising good judgment regarding reasonable personal use, but University management may define 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 may not interfere with work performance or with the University's ability to use its resources for business purposes. Personal use may not violate policies, statutes, contractual obligations, or other standards of acceptable behavior. All personal use shall comply with University regulations.

B. Responsible Use

1. Users shall abide by the University's Ethical Standards and Codes of Conduct.

2. All Users shall protect the University's Restricted and Sensitive Data.

3. All Illegal Behavior is strictly prohibited.

4. Users may not alter Electronic Communications to hide their identity or impersonate another person, including the use of traffic anonymizers (e.g., commercial VPN services, TOR, anonymous proxies).

5. Users may not use University IT Resources, Information Systems, Information Assets, or Electronic Resources for soliciting business, selling

products, or otherwise engaging in commercial activities other than those expressly permitted by University management or other University regulations.

6. Users may 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. Users may not perform actions detrimental to Electronic Resources or that negatively affect other Users' ability to perform their assigned duties. Users may not waste University Electronic Resources or prevent others from using them.

C. Internet Use

1. Users access the internet at their own risk. The University is not responsible for material viewed, downloaded, or received via the internet.

2. To protect personal safety and privacy, internet Users should not give out personal information to others without taking into consideration the risks of doing so.

D. Privacy Expectations

1. Monitoring

a. The University's Information Security Office uses Signature-based Detection and Automated Monitoring activities to ensure compliance with local, state, federal, and University regulations and contractual obligations.

b. The University reserves the right to authorize specific individuals or groups, at times including contracted business partners, to use Signature-based Detection and Automated Monitoring activities to monitor IT Resources, Information Systems, and Electronic Resources to ensure

compliance with local, state, federal, and University regulations and contractual obligations.

2. Privacy of Stored Personal Information and Electronic Communications

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

        i. The University monitors and reviews activities and content on its IT Resources, Information Systems, and Electronic Resources using Signature-based Detection and Automated Monitoring for the purposes of efficiency, security, and operations.

        ii. The University 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 or actions that may be detrimental to the University (e.g., violations of policy). The University 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.

3. Network Access

    a. All University of Utah client networks shall require Users to authenticate via password or other secure authentication mechanisms that allow Users to be uniquely identified.

    b. Any department, college, or other University unit that operates a network shall retain adequate data to allow the University to respond to lawful requests for information by appropriate law enforcement agencies within a reasonable timeframe.

Sections IV- VII 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.

IV. Policies/ Rules, Procedures, Guidelines, Forms, and other Related Resources

A. Policies/ Rules.

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

B. Procedures, Guidelines, and Forms. [*reserved*]

C. Other Related Resources. [*reserved*]

V. References

A. 5 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

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

VI. 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.

VII. History

Revision History

A. Current version. Revision 3.

1. Approved as an Interim Rule by President Randall on September 12, 2023 with effective date of September 12, 2023. Rule finalized with no changes after Board of Trustees approval of Policy 4-004 revisions on November 14, 2023.

2. Legislative History

3. Editorial Revisions

B. Previous versions.

1. Revision 2. Effective date February 1, 2021.

2. Revision 1. Effective date April 4, 2016.

C. Renumbering

1. Not applicable.