Rule R4-004Q: Information Security Policy Sanctions

Revision 0. Effective date: September 12, 2023

I. Purpose and Scope 1

II. Definitions 2

III. Rule 2

A. Cybersecurity Sanctions Matrix 2

IV. Policies/ Rules, Procedures, Guidelines, Forms, and other Related Resources 9

V. References 9

VI. Contacts 10

VII. History 10

I. Purpose and Scope

A. Purpose

The purpose of this Information Security Policy Sanctions Rule is to describe the consequences for violating Policy 4-004 or any associated regulations.

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 Q, titled Violations, of the University of Utah Information Security Policy 4-004.

II. Definitions

The definitions provided in Policy 4-004 apply for this rule.

III. Rule

A. Cybersecurity Sanctions Matrix

Level of Violation	Accidental	Deliberate	Examples of Violations	Actions to be Taken
Level I Errors in handling Restricted or Sensitive Data or in maintaining IT security measures.	• Lack of training • Inexperience • Poor judgement: mistakes made while operating in good faith • Poor process	• Clerical error • Process error • Technical error • Judgement error	• Leaving an active computer unattended which has access to Restricted or Sensitive Data • Accessing Restricted or Sensitive Data which is no longer part of assigned job duties • Failure to complete required cybersecurity training • Failure to report a cybersecurity violation	• Verbal warning and memo of expectations/memo of success • Assigned cybersecurity training • Required review of policy and procedures
Level II Errors in handling Restricted or Sensitive Data or in maintaining	• Curiosity • Concern	• Unauthorized • Non-job related	• Email forwarding and/or the use of an email system that is not approved to	• Written warning, including provisions for mitigation, if appropriate

IT security measures with a disregard for University policy.			conduct University business • Failure to implement appropriate Controls for Restricted or Sensitive Data, either at rest or in transit • Abuse of computer resources administrative privileges • Removal of University IT security tools from University-owned devices • Repeat commission of Level I violations	• Inclusion of expectations/mitigation steps on performance evaluation • Assigned cybersecurity training • Required review of policy and procedures
<u>Level III</u> Breach in the terms of the Confidentiality	• Negligence • Personal/financial gain	• Unauthorized • Disrespect for co-workers,	• Password/Account sharing	• Final written warning, requiring written corrective action plan

Agreement and/or University policies concerning use and disclosure of Restricted or Sensitive Data or in maintaining IT security measures.		supervisor, and patients • Non-job related	• Disregard of University policy and procedure resulting in a breach of Restricted or Sensitive Data • Violation of policy to the extent that organizational harm may result • Storing Restricted or Sensitive Data on an unencrypted storage device • Transmission of Restricted or Sensitive Data resulting in a breach • Disclosure of Restricted or Sensitive Data to co-	or suspension without pay • Suspension of Information System User privileges • Referral to VP as violation of faculty code • Revocation of Medical Staff privileges • Suspension of research projects and inability to participate in research for 12 months • Obligation to make restitution • Possible referral to law enforcement

			workers with no job-related need to know • Using someone else's account through the theft/observation of another employee's credentials • Adding, deleting, or altering Restricted or Sensitive Data without authorization • Posting any Restricted or Sensitive Data on social media that poses harm to the University or individuals it may pertain to	

			• Repeat commission of Level I or II violations	
Level IV Breach in the terms of the Confidentiality Agreement and/or University policies concerning use and disclosure of Restricted or Sensitive Data for personal gain or to affect harm on another person.	• Revenge • Protest • Gross negligence • Dereliction of duty	• Theft, including identity theft • Stealth • Malicious actions: • e.g., alteration or • deletion of data, making Information Systems inaccessible • Willful neglect	• Alteration, deletion, or removal of Restricted or Sensitive Data from University facilities without approval which results in a breach and/or harm to the University and individuals • Unauthorized publication or broadcasting of Restricted or Sensitive Data • Use or disclosure of Restricted or Sensitive Data for illegal purposes	• Termination of employment and ineligible for rehire • Law enforcement engaged • Contract of restitution

			• A pattern of routine security violations due to inattention, carelessness, or a cynical attitude toward security discipline • Repeated Level II or III violations	

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. 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: 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 0.
   1. Approved by President Randall as an Interim Rule 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.

C. Renumbering

1. Not applicable.