Date: August 25, 2023

To: Taylor R. Randall, President

From: Steve Hess, Chief Information Officer
Donna Roach, Chief Information Officer, University of Utah Health
Corey Roach, Chief Information Security Officer

Copies: Jeff Herring, Chair, Institutional Policy Committee
Shanti Deemyad, President, Academic Senate

Subject: Interim Policy 4-004, Interim Rule R4-004A, Interim Rule R4-004C, Interim Rule R4-004D, Interim Rule R4-004F, Interim Rule R4-004G, and Interim Rule R4-004J

Attached please find proposed revisions to the University's Information Security Regulations, including:

- Proposed revisions to the following regulations:
    - Policy 4-004: Information Security Policy
    - Rule R4-004A: Acceptable Use
    - Rule R4-004C: Data Classification and Encryption
    - Rule R4-004D: Access Management
    - Rule R4-004F: Physical and Facility Security
    - Rule R4-004G: IT Resource and Information System Security and Vulnerability Management
    - Rule R4-004J: Log Management and Monitoring
    - Rule R4-004Q: Information Security Sanction Matrix
- Proposed retirement of the following rules:
    - Rule R4-004B: Information Security Risk Management
    - Rule R4-004E: Change Management
    - Rule R4-004H: Remote Access
    - Rule R4-004I: Network Security
    - Rule R4-004K: Backup and Recovery
    - Rule R4-004L: Information System Media Handling
    - Rule R4-004M: Business Continuity and Disaster Recovery
    - Rule R4-004N: Information Security Incident Management
    - Rule R4-004O: Security Awareness and Training.

We request approval of the proposed revisions as an interim policy and interim rules, to take effect immediately upon your approval. We are requesting approval as interim policy so that the University's policies comply with Utah Board of Higher Education Policy [USHE Board Policy](#)

[R345: Information Technology Resource Security](#), which was recently updated, and to immediately strengthen the information security policy to address the present and increasing risks of cyber security incidents. Please indicate your approval by dating and signing this document in the space provided on page 3.

The reasons for the policy revision are as follows:
1. Confront recent cybersecurity issues impacting the university: the data breach reported in spring 2020 (currently under investigation by the Office of Civil Rights) and the ransomware incident in July 2020
2. Meet the cybersecurity goals outlined in Operation Bold Transition, Section XVI (Cybersecurity – Enhance the campus-wide cybersecurity strategy)
3. Address findings from the organizational risk assessment conducted by a third-party firm commissioned by Chief Information Security Officer Corey Roach, as directed by President Randall; the risk assessment's key finding was weak, unenforceable cybersecurity policies at the University of Utah
4. Support the cybersecurity initiative as outlined in President Randall's memo dated January 23, 2023 and Chief Information Security Officer Corey Roach's memo dated May 4, 2023
5. Ensure compliance with the updated [USHE Board Policy R345: Information Technology Resource Security](#)
6. Address the changing cybersecurity threat landscape and risks, in addition to the increasing compliance requirements to which the university is subject

In revising the Information Security Policy and its rules, we sought input from the Department of Internal Audit, the Information Privacy Office, the Office of General Counsel, University Human Resource Management (UHRM), University Information Technology (UIT) Partner Relations, UIT Strategic Communication, University of Utah Hospitals and Clinics Human Resources (UUHC HR), the director for University Regulations, and the Institutional Policy Committee.
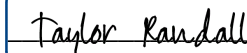
Summary of substantive changes:
- Interim Policy 4-004:
  - Roles and Responsibilities section added with clarity throughout the policy regarding which roles perform specific information security functions and duties in the course of their day-to-day work
  - Vague and ambiguous language removed throughout the policy
  - Section O:
    - Cybersecurity awareness and training is a requirement for all employees
  - Section Q:
    - A Sanctions Matrix has been added
- Interim Rule 4-004C
  - New data type under the Restricted section, Authentication Data
  - Encryption requirements clarified:
    - *"Data at Rest Requirements*
      All devices storing, processing, creating, or transmitting University data, where technically feasible, shall be encrypted."
- Interim Rule 4-004D
  - Authentication services clarified:

- ▪ *"All University IT Resources, IT Systems, and Electronic Resources must use University Information Technology authentication services wherever technically feasible."*
- The following rules will be retired with applicable content moved to the corresponding section in the policy. Aspects of the rules that are instructional in nature will be added to forthcoming procedures:
  - Rule 4-004B: Information Security Risk Management
  - Rule 4-004E: Change Management
  - Rule 4-004H: Remote Access
  - Rule 4-004I: Network Security
  - 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
- The following guidelines will be retired. Current information on the topics contained therein is now included in the proposed policy and rules, or as applicable, articles located on https://it.utah.edu:
  - Guideline G4-004D: Cloud Computing - Opportunities Used Safely
  - Guideline G4-004E: Termination Check List for Information Technology
  - Guideline G-4004J: Vendors and Business Services Agreements
  - Guideline G4-004N1: Media Sanitization and Destruction
  - Guideline G4-004Q: Guidelines for Privacy and Information Security Training and Awareness Contacts (TACs)
  - Guideline G4-004S: Potential Sanctions for Privacy and Security Violations

While it is necessary to promulgate the policy and rules immediately on an interim basis, we plan to finalize the interim regulations through the standard University regulation review and approval process as soon as possible.

Approved this 12th day of September 2023.

DocuSigned by:

Taylor Randall

Taylor Randall, President