University of Utah

Legislative History for

University Rule 4-004A Revision 2, and University Rule 4-004B Revision 2.

As approved by the Academic Senate February 1, 2021, with effective date of February 1, 2021.

Contents:

Summary of changes proposed for 4-004

Addition to Rule 4-004A, no unauthenticated network access

- Reason for this change
    - If a crime is committed on a University IT resource, specifically a network, the University can provide law enforcement with relevant information.
        - ***Only*** if law enforcement provides appropriate documentation.
- Potential impact
    - Negligible for patients, students, non-IT staff and faculty.
    - Some college and departmental IT staff do this already or UIT handles it for them.
    - IT staff who manage their department network are responsible for this information.

Change to Rule 4-004B, removing specific security control framework

- Reasons for this change
    - ISO 27002 (currently listed in the rule) has a cost and is not available to students, faculty, or staff.
    - Alternatives that are as good or more robust include NIST and CIS frameworks at no cost and can be reviewed and downloaded by anyone.
    - NIST frameworks are produced by the US federal government and align with grant requirements from federal or state agencies.
- Potential impact
    - Negligible for patients, students, staff, and faculty.
    - NIST and CIS frameworks have been used widely at the university for many years.

Procedure to clarify the processes in Rule 4-004G (IT Resource and Information System Security and Vulnerability Management)

- Reasons for this change
    - Provide transparency on security staff processes
    - Provide clarity to staff and faculty on Rule 4-004G
- Potential impact
    - Negligible for patients, students, staff, and faculty.

Updated Guideline G4-004B, “Guidelines for Information Security and Privacy Champs”

- Reasons for this change
    - Updates to an outdated guideline (last updated in 2011) that currently references a previous version of the university security policy.
    - Provide clarity regarding the expectations for staff participating in the Security and Privacy (HIPAA) Champs efforts.
- Potential impact
    - Negligible for patients, students, faculty, and staff

To: University of Utah Academic Senate Executive Committee

From: David P. Goldenberg, Senate Advisory Committee on Information Technology Chiar.

Date: 7 January 2021

RE: Proposed changes to University Policy 400-4

Dear Executive Committee,

The Senate Advisory Committee on Information Technology (SACIT) has met with representatives of the University Information Technology (UIT) department on multiple occasions over the past year to discuss proposed additions and changes to the rules and guidelines supporting Policy 400-4. These include:

- Rule 4-004A: Acceptable use (revision)
- Rule 4-004B: Information security risk management (revision)
- Rule 4-004G: Escalation procedure (new rule)
- Guideline G4-004B: Guidelines for Security and HIPAA Champs (revised and renamed)

At its most recent meeting, on 20 November 2020, SACIT endorsed all four of these proposals. In its discussion, there were two major items of concern:

1. In Rule 4-004A III D 2c, the new language regarding client networks:

   > All University of Utah client networks must require users to authenticate via password or other secure authentication mechanisms which allows users to be uniquely identified. It is the responsibility of the department or college operating the network to ensure that adequate information is retained to allow the University to respond to lawful requests for information by appropriate law enforcement agencies within a reasonable timeframe.

   As originally presented to the committee, it appeared that this rule would require a significant investment by many departments to implement password-controlled access to building networks by all computers. At the most recent meeting, however, the committee was assured that "other secure authentication mechanisms" could include physical security of computers in private offices, such as those of faculty members and some staff. The revised rule would require, however, new security measures for computers located in more public spaces. With this clarification, the SACIT endorses the proposed rule change.

2. In Rule 4-004B, III B:

   > The University leverages numerous government and industry recognized information security control frameworks depending on the situation,risk tolerance, data types,and as specified in applicable regulations.

The original proposal included language referring to a specific set of US government standard, National Institutes of Standards (NIST) 800-53. After concerns were raised about the applicability of this standard to all university systems, UIT changed the proposal to include the more general language shown above.

As presently written, and with the understandings described above, SACIT fully endorses the proposed rules and guidelines.

Respectfully yours,

David P. Goldenberg

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

. 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.

    c. All University of Utah client networks must require users to authenticate via password or other secure authentication mechanisms which allows users to be uniquely identified. It is the responsibility of the department or college operating the network to ensure that adequate information is retained to allow the University to respond to lawful requests for information by appropriate law enforcement agencies within a reasonable timeframe.

[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, FORM, and OTHER RELATED RESOURCES

A. Rules

TBD

B. Procedures

Policy 4-004 Procedures

C. Guidelines

TBD

D. Forms

E. Other Related Resources

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

C. 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:

D. "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.... "

E. "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

RULE 4-004B INFORMATION SECURITY RISK MANAGEMENT, REV. 1

I. PURPOSE AND SCOPE

A. The purpose of this Information Security Risk Management Rule is to establish the University's risk management program. The objective of University's Risk Management Program is to support University's core institutional and research missions as well as patient safety and quality of care goals, while also mitigating financial, operational, reputational and regulatory compliance risk. This Information Security Risk Management Rule shall enable the University to accomplish its missions by:

1. Securing the Information Systems that create, maintain, process, or transmit University data designated as "Restricted" or "Sensitive" per the University's Data Classification and Encryption Rule.

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

B. This Rule supports section B, titled Information Security Risk Management, 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. **Confidential -** Any Information Asset which is classified as Restricted or Sensitive per the Data Classification and Encryption Rule.

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

C. **Restricted Data** - Any data types classified as Restricted per the Data Classification and Encryption Rule.

D. **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.

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

F. **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

A. The University's information security risk management methodology is based foremost on the National Institute of Standards and Technology (NIST) Special Publication 800-30 "Risk Management Guide for Information Technology Systems" methodology.

B. The University~~'s~~ leverages numerous government and industry recognized information security control frameworks ~~is based foremost on the Internal Organization for Standardization (ISO) 27002:2013 control framework and additionally incorporates other relevant control requirements tailored to the University's~~ depending on the situation, risk tolerance, data types, and as specified in applicable regulations.

a. For questions regarding information security control frameworks and what is applicable to the situation in question, please contact the Information Security Office at iso-grc@utah.edu or ciso@utah.edu

C. Risk Assessment

a. Inherent risk scores are calculated based on the following five (5) vectors of risk, which assess both the likelihood and impact of compromise:

a. Impact: The number of Users who access the Information System

b. Impact: The number of individual data records stored on the Information System

c. Likelihood: The type of architecture that Information System employs

d. Likelihood: The types of Users that access the Information System

e. Likelihood and Impact: The highest classification of data the Information System creates, maintains, processes, or transmits

b. Residual risk scores are calculated based on the inherent risk score and the percentage of compliance of the control objectives assessed during a full risk assessment. A full risk assessment includes the following elements:

. Entity level controls

a. System level controls

D. Risk Management

The appropriate University key stakeholders shall be issued both Inherent and Residual Risk scores in risk assessment summary reports for all Information Systems assessed. These stakeholders will be responsible for either formally accepting the risk of operating the Information System in the University's environment, or rejecting the risk and requiring a formal corrective action plan to allocate the appropriate timelines, budget line items, and/or other resources to remediate control failures and reduce the Residual Risk score to an acceptable level for the University.

[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, FORM, and OTHER RELATED RESOURCES

A. Rules

TBD

B. Procedures

Policy 4-004 Procedures

C. Guidelines

TBD

D. Forms

E. Other Related Resources

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

N. Cyber Security Framework: The Cyber Security Framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

VI. CONTACTS

A. 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

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

Note: this is not a revision or a replacement of an existing procedure.

University Procedure supporting Rule 4-004G

I. PURPOSE AND SCOPE:

A. The purpose of this Procedure is to outline the Information Security Office (ISO) team's process for the notification and escalation of exceptions to policy and or known vulnerabilities.

B. This Procedure supports sections:
   a. III.C, titled Vulnerability Management, of Rule 4-004G: IT Resource and Information System Security and Vulnerability Management.
   b. III.P, titled Exceptions to Policy, of Policy 4-004 University of Utah Information Security Policy.

II. DEFINITIONS:

All terminology referenced in this Procedure is defined in Policy 4-004: University of Utah Information Security Policy. All defined terms are capitalized within this Procedure.

A. 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.

B. Asset - Any University-owned Information Asset or IT Resource that is a part of University business processes

C. Urgent – The "Urgent" classification applies to broad threats to the University or remotely exploitable vulnerabilities through which an intruder can easily gain control of numerous Information Systems, gain full read and write access to files, remotely execute commands, exploit backdoors, or cause wide-spread service interruption. Intruders can easily gain control of the host, which can lead to the compromise of the University's entire network security. Vulnerabilities assigned a rating of "Urgent" must be remediated within 72 hours of discovery.

D. Critical – The "Critical" classification applies to vulnerabilities through which an intruder can possibly gain control of one or more Information Systems, gain full read access to files, potential backdoors, a listing of all the users on the host, or there may be potential leakage of Confidential information. This includes local exploits where the risk of compromise is not as high as an Urgent vulnerability. Vulnerabilities assigned a rating of "Critical" must be remediated within 15 days of discovery.

E. Serious – The "Serious" classification applies to vulnerabilities that may allow an intruder to gain access to a partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying. Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. Vulnerabilities assigned a rating of "Serious" must be remediated within 30 days of discovery.

F. Medium – The "Medium" classification applies to vulnerabilities that may allow an intruder to gain access to Information Assets stored on an Information System, or collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions. Vulnerabilities assigned a rating of "Medium" must be remediated within 60 days of discovery.

G. Low – The "Low" classification applies to vulnerabilities that do not pose an immediate threat to the University Information Systems. Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities. Vulnerabilities assigned a rating of "Low" should be remediated within 90 days of discovery.

III. PROCEDURE:

A. ISO receives notification of the need for exception to policy.
   1. ISO requests current vulnerability scan to determine vulnerabilities present on the Asset/s.
   2. The results of the vulnerability scan will determine the timeline for remediation or exception to policy.

B. The IT Technician is notified via email of the need for exception to policy and vulnerabilities existing on the Asset/s.
   1. ISO will document every attempted communication with IT Technician and all concerned parties
   2. For vulnerabilities classified as Urgent, remediation or exception to policy must be submitted to ISO within 72 hours of discovery.
   3. For vulnerabilities classified as Critical, remediation or exception to policy must be submitted to ISO within 15 days of discovery.
   4. For vulnerabilities classified as Serious, remediation or exception to policy must be submitted to ISO within 30 days of discovery.
   5. For vulnerabilities classified as Medium, remediation or exception to policy must be submitted to ISO within 60 days of discovery.
   6. For vulnerabilities classified as Low, remediation or exception to policy must be submitted to ISO within 90 days of discovery.

C. In the event IT Technician has not responded to communications from ISO within 50% of the time allowed for remediation or exception to policy the following shall occur.
    1. IT Technicians direct supervisor will be informed of current situation and required action/s.

D. In the event direct supervisor and/or IT technician have not responded to communication from ISO within 75% of the time allowed for remediation or exception to policy the following shall occur.
    1. Director level or above shall be informed of current situation and required action/s.

E. In the event no communication is received by ISO and the time allowed for remediation or exception to policy has lapsed the following shall occur.
    1. On approval from the Chief Information Security Officer (CISO), the asset may be removed from the University of Utah network space through appropriate means.
    2. An email will be sent to concerned parties documenting all communication attempts and relevant University Policies.
    3. Asset may not be permitted access to University of Utah network space until required remediation or exception to policy is completed.

F. If at any time ISO determines that the Asset remaining on the network represents an unacceptable level of risk to the University of Utah and on approval from the Chief Information Security Officer (CISO) the Asset may be removed until such time as vulnerabilities are remedied.

[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

B. Procedures

C. Guidelines

D. Forms

E. Other related resources materials

V. References

A. Policy 4-004: Information Security Policy

VI. Contacts

The designated contact officials for this Procedure are:

A. Procedure Owner (primary contact person for questions and advice): Trevor Long (trevor.long@utah.edu) or ISO-GRC (ISO-GRC@utah.edu)
B. Policy Officer: Chief Information Security Officer

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: 1.0, effective date: November 1, 2020

THE UNIVERSITY OF UTAH®

Title:	Guidelines for ~~Information~~ Security and ~~Privacy Liaisons~~ HIPAA Champs
Number:	G4-004B
Responsible Office:	Information Security Office and Privacy Office ~~(IPSO)~~
Last Revision:	January ~~2011~~ 2020
Owner:	~~Director, ISPO. 801-587-9241 it_policy@utah.edu~~ Chief Information Security Officer (CISO), 801-58x-xxxx, ciso@utah.edu

---

I. OVERVIEW

a. This guideline is meant to provide procedures, standards, and other guidance for the implementation of University ~~Policy 4-004: The University of Utah Information Security Policy – Section B (1): Information Security Liaisons~~ Rule 4-004O, Information Security Awareness and Training.

II. GUIDELINES

a. ~~Information~~ Security Champs and ~~Privacy Liaisons (ISPLs)~~ HIPAA Champs serve as points of contact between academic, administrative, clinical, and research units and the Information Security Office and Privacy Office (ISO and PO respectively) for all matters relating to information security and privacy. ~~An ISPL coordinates with the Information Security and Privacy Office to implement the University's information security and privacy policies and procedures.~~ Specifically, this role is intended to:

i. Promote information security/privacy awareness and ~~good security~~ best practices.
ii. ~~When possible,~~ Attend ~~information security~~ awareness and training presentations, seminars, workshops and events related to information security/privacy on at least a quarterly basis.
iii. Disseminate~~s~~ information provided by the ISP~~O~~ and PO ~~within the department to raise awareness about information security issues~~ to their respective units.
iv. Participate in~~,~~ and support ~~the establishment of,~~ information security/privacy incident response and reporting processes~~, including incident reporting~~.
v. ~~Provide oversight~~ Collaborate with the ISO to develop and implement ~~for the~~ security measures related to their unit's ~~of the department's~~ information systems.
vi. ~~Coordinate~~ Work with ISO to develop an ~~inventories~~ inventory of their unit's restricted and sensitive ~~or critical~~ information and, the unit's information systems.
vii. ~~Coordinate~~ As required, assist with information security/privacy risk assessments.
viii. ~~Coordinate business continuity planning.~~ As required, participate in implementing corrective action plans related to information security/privacy.
ix. ~~Assist in implementing corrective action plans resulting from examination or investigation of an incident report.~~ Promote University policies and procedures related to information security/privacy.
~~x. Document the department's security standards and plans.~~
~~xi. Bolster the role of the Information Security and Privacy Training and Awareness Contact ("TAC"):~~
~~1. Ensure that the TAC conducts training activities to promote security awareness and good security practices.~~

~~2. Ensure that the TAC disseminates information provided from ISPO within the department to raise awareness about information security issues.~~

b. The Information Security Office and Privacy Office will provide training and resources to the ~~Liaison~~ Security and HIPAA Champs on at least a ~~routine~~ quarterly basis, and will ~~prioritize calls and other communications from the Liaison~~ provide additional support as needed.

~~c. For a list of assigned Information Security and Privacy Liaisons, see the University's Information Security web site at http://www.secureit.utah.edu~~