University Procedure 4-004G: supporting Rule 4-004G

Revision 0. Effective date: February 1, 2021

I. Purpose and Scope

A. Purpose: 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. Scope:

This Procedure supports sections:

1. III.C, titled Vulnerability Management, of Rule 4-004G: IT Resource and Information System Security and Vulnerability Management.
2. 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

V. References

VI. Contacts

The designated contact officials for this Regulation are

A. Procedure Owner (primary contact person for questions and advice): Associate Director – Governance, Risk, & Compliance, 801-587-2210

B. Policy Officers: Chief Information Security Officer, 801-213-3397

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 provide 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 who 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

Renumbering: None

Revision History:

Current version: Revision 0

Approved by Academic Senate February 1, 2021

Effective Date February 1, 2021