Procedure P4-004P: Exceptions to Policy

Revision 0. Effective date: November 6, 2024

I. Purpose and Scope

A. Purpose.

The purpose of this Exceptions to Policy Procedure is to outline the process for seeking exceptions to Policy 4-004 and its associated regulations.

B. Scope.

The scope of this procedure 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 procedure supports Section P, titled Exceptions to Policy, of the University of Utah Information Security Policy 4-004.

II. Definitions

The definitions provided in Policy 4-004 apply for this procedure. In addition, the terms below apply for the limited purpose of this procedure.

A. Business Impact Analysis (BIA) – A detailed examination of an Asset's requirements, function, and interdependencies used to characterize Asset contingency requirements and priorities in the event of a significant disruption.

B. GRC – The Information Security Office's Governance, Risk & Compliance team. Contact: ISO-GRC@utah.edu.

C. Requester – The owner of the Information System requiring an exception to policy.

D. Signatories – The approvers of exception to policy requests, including the chief information security officer (CISO), chief technology officer (CTO), and the cognizant vice president, dean, or other person in a position of similar seniority able to accept Risk on behalf of the University.

III. Procedure

A. Requesting an Exception to Policy

1. An exception to policy may be requested by the owner of the Information System needing an exception to policy (the Requester) through the GRC team.

2. The Requester shall provide the exception to policy request details, BIA, and mitigating Controls in place to reduce Risk and have a plan for becoming compliant.

3. GRC shall review the information, work with the Requester to identify associated Risks, and provide a recommendation to the Signatories on whether to approve the exception to policy request based on an analysis of the mitigating Controls and Risks.

B. Approval of an Exception to Policy

1. The Requester is responsible for obtaining approval from the cognizant vice president, dean, or other person in a position of similar seniority able to accept Risk on behalf of the University for their department.

2. GRC shall submit the exception to policy request to the CISO and CTO for their approval.

3. If approved, an exception to policy is valid for one year from the date signed by the Signatories.

4. GRC shall maintain a copy of the approved exception to policy request on file and provide a copy to the Requester and each Signatory.

C. Denial of an Exception to Policy

1. An exception to policy request may be denied by any Signatory.

2. The Requester may appeal the denial of an exception to policy request to the cognizant chief information officer (CIO).

D. Renewing or Retiring an Exception to Policy

1. Prior to an approved exception to policy expiring, the Requester shall contact GRC and state whether the exception to policy is still needed or can be retired.

2. The Requester shall update the exception to policy request details, BIA, and mitigating Controls, as applicable.

3. GRC shall review the updated information, work with the Requester to identify any additional Risks, and provide an updated recommendation to the Signatories on whether to renew the exception to policy request based on an analysis of the mitigating Controls and Risks.

Sections IV- VII are for user information about this procedure.

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

A. Policies/ Rules.

1. Policy 4-004: University Information Security Policy

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

C. Other Related Resources.

V. References

[*reserved*]

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 Chief Information Security Officer with effective date of November 6, 2024.

B. Renumbering

1. Not applicable