Effective: *08/08/2022*
Last Revised: *03/19/2025*

Responsible University Administrator:
Assistant Vice President, IT Security Services

Responsible University Office:
Information Technology Services

Standard Contact:
IT Security Services
security@nebraska.edu

ITS-01: Policy Exception Standard

Standard Contents

1. Purpose

The purpose of the Policy Exception Standard is to define the organization's requirements for enforcing effective policy exception management.

The University of Nebraska System ("University") is committed to safeguarding its information and computing infrastructure upon which the teaching, research, community service, and healthcare functions rely. Additionally, the University is strongly committed to maintaining the security and privacy of confidential personal information and other data it collects or stores.

To guide the University community in achieving these objectives, the University has established policies, standards, and procedures that all users are required to follow. However, the University also recognizes that there may be academic and research pursuits that require deviations from these policies, standards, and procedures. Therefore, the University has developed an exceptions process that users may utilize to justify such deviations and document the associated risks.

2. Scope

This standard applies to all University ITS standards and technology assets. Any information not specifically identified as the property of other parties, that is transmitted or stored on Information Systems (including email, messages, and files) shall be considered the property of the University and to which this standard applies. All users (employees, contractors, vendors, or others) of Information Systems are responsible for adhering to this standard.

3. Standard Statement

It is the intention of this Standard to establish a policy exception process throughout the University to help the organization implement security best practices. The following subsections outline the Policy Exception Standard.

Only information systems that are compliant with University IT Policies, Executive Memoranda, Standards, Controls, Procedures and/or Information Systems that have received exceptions through this process shall be covered by the University insurance policies, including cyber security.

4. Policy Exception Requirements

4.1 Exception Requirements

Any exception request for a specific Policy, Executive Memorandum, Standard, Control, or Procedure section/control must provide the following information relevant to the request:

- IT requestor's name, email address, and department.
- User's name, email address, and department.
- The User's organizational leadership's name and email address.
- The User's dean or director name and email address.
- Complete a Risk Classification Self-Assessment for the Information System and data for which the exception is requested.
- Specify the Policy, Executive Memorandum, Standard, Control, or Procedure section(s) and/or control(s) for which an exception is requested.
- List of users, Information Systems, and data for which the exception will apply.
- Academic, research, or business justification for why the exception is requested.
- Alternative technical or process solutions that could be implemented in place of a policy exception, and why the alternatives are not feasible.
- Details on the mitigations and compensating controls the requestor will take to secure the Information System or data, if an exception is approved.
- Term for which the exception is requested (three, six, or twelve months).

4.1.1 IT Security Team
University information security policies, standards, procedures, guidelines, and services are managed through the ITS Security team. The ITS Security team will review each exception request to assess eligibility with known regulations and compliance frameworks and determine whether appropriate compensating security controls are present or can be reasonably implemented to mitigate the risk the exception presents to the operation of Information Systems introduced by removing primary security controls.

4.1.2 University Research Offices
Each Campus Research Office is responsible for ensuring campus research is conducted according to University policies and standards, as well as ensuring compliance with all required contractual requirements, regulations, and compliance frameworks. Exception requests that impact research information systems or data will be reviewed by the Campus Research Office to determine eligibility.

4.1.3 IT Security Exception Standing Committee
The IT Security Exception Standing Committee will consist of a diverse group of professionals from ITS, Distributed IT, and University Research representing organizations across the University System. The committee serves at the discretion of the AVP for IT Security, and the committee will provide recommendations to Exception Approvers when the impact of an exception request cannot be appropriately mitigated by compensating security controls implemented by ITS Security Services or responsible IT professionals.

4.1.4 Exception Approvals
The Office of the Vice President of Information Technology, in collaboration with the Office of the Vice President and General Counsel, will assess the level of risk associated with the proposed exception. The magnitude of the assessed risk will dictate the level of approval that is required. After the request has been conditionally approved by a department chair or business officer, the details will be confirmed by the IT Security Exception Standing Committee. Final review and the level of approval required is based on the following chart:

Risk associated with exception	Department Chair/Business Officer and Campus CIO	Dean/Division Leader and AVP for IT Security	VC/VP and VP for IT
Low Risk	X		
Medium Risk	X	X	
High Risk	X	X	X

University leaders, including academic deans, academic chairs, vice chancellors, and vice presidents, may not approve their own exception requests. It is incumbent upon the next higher level authorizing official to review and decide upon an exception.

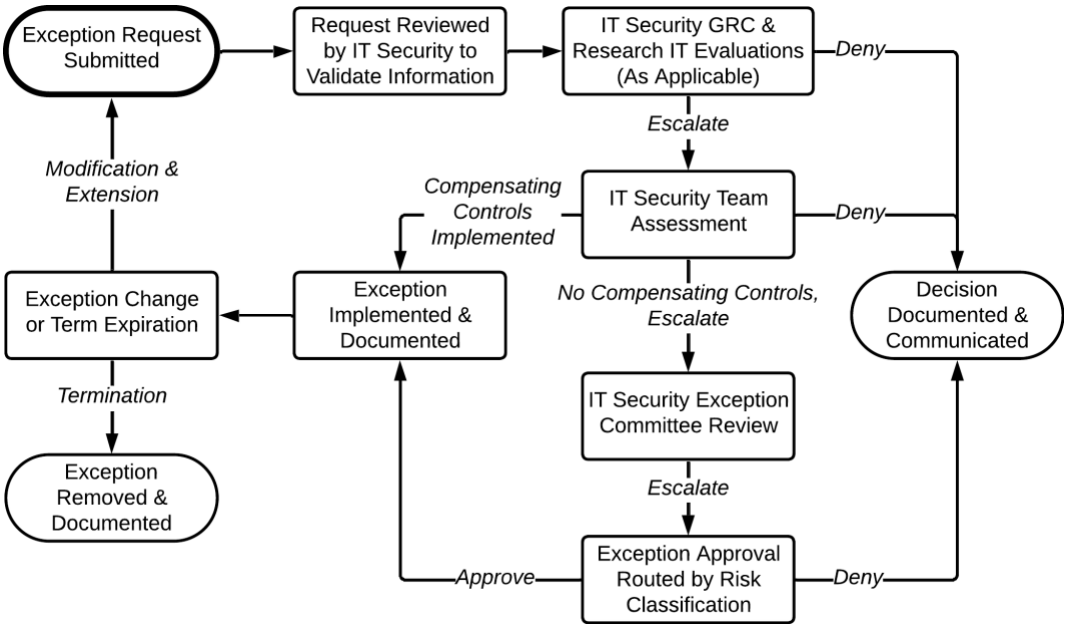
4.1.5 Exception Scope
Exceptions will not be granted when feasible alternatives exist, or risks outweigh projected benefits.

Exceptions will not be granted if the information system or data is covered by contractual requirements, regulations, or compliance frameworks outside of the University.

If a policy exception is granted, it is granted for the current state of the information system and/or process/use-case. If the information system or process is replaced, modified, expanded, or altered, the current exception is null and void, and a new exception will need to be requested, reviewed, and approved.

4.2 Exception Processes

The following diagram summarizes the Exception Processes detailed in sections 4.2.1 through 4.2.4.



4.2.1 Initial Exception Request

Any university IT employee can initiate a policy exception request for themselves or a user they support by using the **IT Policy Exception** request form. The form guides requestors through the policy exception process as follows:

1. Using the **IT Policy Exception** request, the requestor enters the required information into the fields provided. Requestors may also upload relevant supporting documentation.

2. Once the request is submitted, it is assigned to the accountable user for confirmation and authorization to proceed to the University Research Office and/or IT Security Team for review.

3. If the exception request includes an information system or data aligned with University research, the Campus Research Office will determine eligibility with all in-scope contractual requirements, regulations, and compliance frameworks before proceeding to the IT Security Team for review. If the Campus Research Office determines that the exception request conflicts with contractual requirements, regulations, or compliance frameworks, the requestor will be informed via email with a documented denial of the request, along with the request details.

4. The IT Security Team (and any additional security control assessors) coordinate with the requestor to accomplish the following:
   a. Assess and document the risks created by the exception.
   b. Assess eligibility with known regulations or compliance frameworks.
   c. Evaluate and document potential alternatives to the exception.
   d. Identify and document potential compensating controls and risk mitigations for the exception.
   e. Document the IT Security Team's assessment of the request.

5. The IT Security Team will vote on the exception request, requiring a minimum of three votes to implement an exception or two votes to escalate an exception for review by the IT Security Exception Standing Committee.
    a. If the IT Security Team determines that the exception request conflicts with known regulations or compliance frameworks, the requestor will be informed via email with a documented denial of the request, along with the request details.
    b. If compensating controls provide appropriate protection and follow known regulations and compliance frameworks, the IT Security Team will approve the exception and move to implementation.
    c. If compensating controls do not provide appropriate protection or are unavailable, the IT Security Team will escalate the exception request.

6. The Security Exception Standing Committee will review escalated exception requests and provide Exception Approvers with a summary recommendation that will contain the following information:
    a. Original exception request submission and any follow-up communication with the requestor.
    b. NU Risk Classification for the information system and data in scope.
    c. Required Exception Approvers.
    d. A summary of the exception request.

    The Security Exception Standing Committee will route the exception request for signatures (including additional supporting documentation) through the appropriate approval path defined in section 4.1.4.

7. Exception Approvers review the recommendation provided by the IT Security Exception Standing Committee.
    a. Low Risk exceptions require approval by both a Department Chair/Business Officer and the Campus CIO.
    b. Medium Risk exceptions require approval by Low Risk approvers and the Dean/Division Leader and the AVP for IT Security.
    c. High Risk exceptions require approval by Low Risk and Medium Risk approvers, and the VC/VP and VP for IT.
    d. Exception approval requires unanimous agreement by identified risk approvers and documented acceptance by the IT requestor and the accountable user. If unanimous agreement is not possible, the exception will not be granted.

8. If the exception is granted and approvals obtained:
    a. The IT Security Exception Standing Committee will inform the requestor via email with documented approval of the request, along with the request details.
    b. The IT Security Exception Standing Committee will verify compliance of the exception with the requestor and relevant data steward(s) or other individual(s) who have a role in fulfilling the exception request.
    c. Notification of approval and all documentation is sent to immediate supervisor, department head/Chair, Dean, and vice chancellor/vice president.
    d. Notification of approval and all documentation is sent to NU Legal.
    e. Notification of approval and all documentation is sent to Risk Management.
    f. Notification of approval and all documentation is sent to data stewards, when applicable.
    g. Notification of approval and all documentation is sent to campus CIO, AVP for IT Security, and VP for IT.
    h. The requestor will be notified prior to the expiration that the exception duration is ending. The requestor must then submit a new exception request or notify IT Security Services that the exception is no longer required.

9. If the exception is not granted:
    a. The IT Security Exception Standing Committee will inform the requestor via email with a documented denial of the request, along with the request details.
    b. Notification of denial and all documentation is sent to the immediate supervisor, department head/Chair, Dean, and vice chancellor/vice president.
    c. The IT Security Exception Standing Committee will work with the requestor to define a reasonable deadline for compliance. The requestor may appeal the decision to the Vice President for Information Technology.

4.2.2 Exception Modification

When a modification in state occurs for an Information System and/or process/use-case or a change in risk classification occurs, the requestor must notify the IT Security Team through the IT Policy Exception request form to reevaluate the exception. When a change occurs with a University IT Policy, Executive Memorandum, Standard, Control, or Procedure that impacts an approved exception, the IT Security Team will notify the requestor to start reevaluating the exception through the IT Policy Exception request form.

4.2.3 Exception Extension

When an approved exception is 60 days from expiration, the requestor will be notified by email so they may request an extension or terminate the exception if it is no longer required. A requestor may submit an exception extension up to 21 days before the expiration of the current extension. Requestors can initiate a policy exception extension request using the IT Policy Exception request form, which guides requestors through the policy exception process as detailed in section 4.2.1.

4.2.4 Exception Termination

When the requestor determines that an approved exception is no longer necessary, they will promptly notify the IT Security Team via email or a support request to remove any implemented compensating controls, mitigations, or other configurations. If a change occurs related to a University IT Policy, Executive Memorandum, Standard, Control, Procedure, external contractual requirement, regulation, or compliance framework, the IT Security Team will inform the requestor to coordinate the removal of any implemented compensating controls, mitigations, or other configurations.

5. Procedures

Procedures specific to this Standard are to be documented and maintained by the individual service owners throughout the University system.

6. Compliance

Compliance Measurement
The University of Nebraska IT Security Services team will verify compliance to this Standard through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Standard owner.

Non-Compliance
Failure to comply with University IT standards may result in sanctions relating to the individual's use of IT resources or other appropriate sanctions according to policies applicable to University faculty and staff or student conduct.

7. Related Information

The following is a listing of related Policies, Executive Memoranda, Standards, Controls, and Procedures.

NIST 800-53
NIST 800-171
NU Executive Memorandum 16
NU Executive Memorandum 26
NU Executive Memorandum 41
NU Executive Memorandum 42

University-Wide Policies & Guidelines - https://nebraska.edu/offices-policies/policies
ITS-00 Information Technology Definitions and Roles
ITS Knowledge Base - https://uofnebraska.sharepoint.com/sites/NU-ITS/KB

8. Approvals and Revision History

Approval of this Standard:

	Name	Title	Date
Authored by:	Richard Haugerud	IT CISO	3/19/2025
Approved by:	Bret Blackman	IT CIO	3/19/2025

Revision history of this Standard:

Version	Date	Description
1.0	08/08/2022	Initial Standard Published
1.1	01/05/2024	Updated 4.1 Exception Requirements and 4.2 Exception Process to establish an updated request workflow facilitated by an IT employee for a supported user. Removed 4.5.1 Threat Event Assessment.
1.2	10/09/2024	Updated 4.5 Exception Recommendation Process with a more efficient workflow.
1.3	03/19/2025	Updated 4.1 Exception Requirements and 4.2 Exception Processes to establish a more efficient workflow with a new distributed responsibility model between the IT Security Team, University Research Offices, IT Security Exception Standing Committee, and Exception Approvers. Merged sections for Exception Modification, Exception Extension, and Exception Recommendation Processes into 4.2 Exception Processes.