ITS-01: Policy Exception Standard

Standard Contents
1. Purpose ........................................................................................................................................... 2
2. Scope .............................................................................................................................................. 2
3. Standard Statement ......................................................................................................................... 2
4. Policy Exception Requirements ....................................................................................................... 2
    4.1 Exception Requirements ............................................................................................................. 2
    4.2 Exception Process ....................................................................................................................... 3
    4.3 Exception Modification Process .................................................................................................. 4
    4.4 Exception Extension Process ....................................................................................................... 4
    4.5 Exception Recommendation Process .......................................................................................... 5
5. Procedures ......................................................................................................................................... 8
6. Compliance ......................................................................................................................................... 8
7. Related Information ............................................................................................................................ 9
8. Approvals and Revision History ..................................................................................................... 9
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 user who wishes to be granted an exception from a specific Policy, Executive Memorandum, Standard, Control, or Procedure section/control must provide the following information relevant to the request:

- Requestor’s name, email address, and department.
- Immediate supervisor’s name and email address.
- Department Chair’s name and email address (if different from immediate supervisor)
- Dean’s name and email address (if different from immediate supervisor)
- If applicable, the requestor’s technical support person(s) name(s) and email address(es).
- Specify the Policy, Executive Memorandum, Standard, Control, or Procedure section(s) and/or control(s) for which an exception is requested.
- Complete a Risk Classification Self-Assessment for the Information System and data for which the exception is requested.
- List of Information Systems and data for which the exception will apply. The list must include uniquely identifiable information such as the fully qualified name of any Information Systems (e.g., abc.nebraska.edu) and the data classification (e.g., high, medium, or low).
- Business justification for why the exception is being requested.
- Describe the steps that 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 IT Security Exception Standing Committee
The IT Security Exception Standing Committee will consist of a diverse group of IT professionals from ITS and Distributed IT representing organizations across the University System. The committee serves at the discretion of the AVP for IT Security and the committee will provide recommendations based on the impact of IT Policies, Executive Memoranda, Standards, Controls, Procedures, and the risk the exception presents to the operation of Information Systems.

4.1.2 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:

<table>
<thead>
<tr>
<th>Risk associated with exception</th>
<th>Department Chair/Business Officer and Campus CIO</th>
<th>Dean/Division Leader and AVP for IT Security</th>
<th>VC/VP and VP for IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Risk</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium Risk</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>High Risk</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

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.

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

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 Process
Any University employee can initiate a policy exception request by using the IT Policy Exception request form. Requests must be submitted by the individual that requires the exception and not by a third party or proxy, including support personnel. 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 requestor’s department chair/business officer for conditional approval.

3. If conditional approval is granted, the request is assigned to the IT Security Exception Standing Committee for review.

4. The IT Security Exception Standing Committee (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. Identify potential risk mitigations for the exception.
   c. Evaluate and document potential alternatives to the exception.
   d. Document the IT Security Exception Standing Committee’s recommendation for approvers.
   e. Route the exception request for signatures (including additional supporting documentation) through the appropriate approval path defined in section 4.1.2.
5. 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. If unanimous agreement is not possible, the exception will not be granted.

6. 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.

7. If the exception is not granted:
   a. The IT Security Exception Standing Committee will inform the requestor via email with documented denial of the request, along with the request details.
   b. Notification of denial and all documentation is sent to 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.

4.3 Exception Modification Process

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 Exception Standing Committee 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 Exception Standing Committee will notify the requestor to start reevaluating the exception through the IT Policy Exception request form.

4.4 Exception Extension Process

When an approved exception is 60 days from expiration, the IT Security Exception Standing Committee will notify the requestor by email so that the requestor 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 by using the IT Policy Exception request form, which guides requestors through the policy exception extension process as follows:

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

2. Once the request is submitted, it is assigned to the requestor’s department chair/business officer for conditional approval.
3. If conditional approval is granted, the request is assigned to the IT Security Exception Standing Committee for review.

4. The IT Security Exception Standing Committee (and any additional security control assessors) coordinate with the requestor to accomplish the following:
   a. Assess and document the risks created by the exception extension.
   b. Identify potential risk mitigations for the exception extension.
   c. Evaluate and document potential alternatives to the exception extension.
   d. Document the IT Security Exception Standing Committee’s decision for the extension request.

5. If the exception extension is granted:
   a. Low Risk Extensions: Notification of approval and all documentation is sent to immediate supervisor, department chair/business officer and the campus CIO.
   b. Medium Risk Extensions: Notification of approval and all documentation is sent to immediate supervisor, department chair/business officer, dean/division leader, campus CIO, and the AVP for IT Security.
   c. High Risk Extensions: Notification of approval and all documentation is sent to immediate supervisor, department chair/business officer, dean/division leader, campus VC/VP, campus CIO, AVP for IT Security, and VP for IT.
   d. 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.

6. If the exception extension is not granted:
   b. The IT Security Exception Standing Committee will inform the requestor via email with documented denial of the request, along with the request details.
   c. Notification of denial and all documentation is sent to immediate supervisor, department head/Chair, Dean, and vice chancellor/vice president.
   d. 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 Assistant Vice President for IT Security.

4.5 Exception Recommendation Process

The IT Security Exception Standing Committee will provide Exception Approvers with a structured recommendation for each policy exception request. Each recommendation will include appropriate alternatives, mitigations, and an Overall Risk Assessment for the requested exception. Each recommendation will contain the following information:

- Original exception request submission and follow-up communication.
- NU Risk Classification for the Information System in scope.
- Required Exception Approvers.
- A summary of the exception request.
- Technical alternatives and mitigation options.
- Process alternatives and mitigation options.
- Overall Risk Assessment score.

Risk assessments will align with NIST SP800-30 Guide for Conducting Risk Assessments to determine an Overall Risk Assessment score for an exception request. Each risk assessment measures the likelihood of occurrence and the impact level of a potential threat event for the information system or data in scope of the exception request.
4.5.1 Threat Event Assessment
A threat event is any possible event which may cause a loss of confidentiality, integrity, or availability of an information system or the data it transmits, processes, or stores.

- **Loss of Confidentiality**
  Definition: Confidentiality [44 U.S.C., Sec. 3542] - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Examples include:
  - The system and its data are compromised by threat actors.
  - The system and its data are released publicly without approval.
  - The system and its data erroneously publish data on public-facing portions of the system (i.e., web page) without authorization.

- **Loss of Integrity**
  Definition: Integrity [44 U.S.C., Sec. 3542] - Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. Examples include:
  - The information system and its data can no longer be trusted.
  - The information system and its data are not complete or is incorrect.

- **Loss of Availability**
  Definition: Availability [44 U.S.C., Sec. 3542] - Ensuring timely and reliable access to and use of information. Examples include:
  - The information system and its data experience a hardware or software failure.
  - The information system and its data are no longer accessible by authorized users.

4.5.2 Likelihood of Occurrence Assessment
The likelihood of occurrence is a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities. [CNSSI No. 4009, adapted]

- **Very High (Qual) / 96-100 or 10 (Semi-Quant)**
  - Error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year.
  - If the threat event is initiated or occurs, it is almost certain to have adverse impacts.

- **High (Qual) / 80-95 or 8 (Semi-Quant)**
  - Error, accident, or act of nature is highly likely to occur; or occurs between 10-100 times a year.
  - If the threat event is initiated or occurs, it is highly likely to have adverse impacts.

- **Moderate (Qual) / 21-79 or 5 (Semi-Quant)**
  - Error, accident, or act of nature is somewhat likely to occur; or occurs between 1-10 times a year.
  - If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts.

- **Low (Qual) / 5-20 or 2 (Semi-Quant)**
  - Error, accident, or act of nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years.
  - If the threat event is initiated or occurs, it is unlikely to have adverse impacts.

- **Very Low (Qual) / 0-4 or 0 (Semi-Quant)**
  - Error, accident, or act of nature is highly unlikely to occur; or occurs less than once every 10 years.
  - If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts.
4.5.3 Impact Level Assessment
The impact level is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. [CNSSI No. 4009]

- **Very High (Qual) / 96-100 or 10 (Semi-Quant)**
  The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.

- **High (Qual) / 80-95 or 8 (Semi-Quant)**
  The threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

- **Moderate (Qual) / 21-79 or 5 (Semi-Quant)**
  The threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

- **Low (Qual) / 5-20 or 2 (Semi-Quant)**
  The threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

- **Very Low (Qual) / 0-4 or 0 (Semi-Quant)**
  The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.
4.5.4 Overall Risk Assessment

The Overall Risk Assessment is equal to the highest risk level for any calculated potential threat event outcome.

- **Very High (Qual) / 96-100 or 10 (Semi-Quant)**
  Very high risk means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.

- **High (Qual) / 80-95 or 8 (Semi-Quant)**
  High risk means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

- **Moderate (Qual) / 21-79 or 5 (Semi-Quant)**
  Moderate risk means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

- **Low (Qual) / 5-20 or 2 (Semi-Quant)**
  Low risk means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

- **Very Low (Qual) / 0-4 or 0 (Semi-Quant)**
  Very low risk means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

### Risk Level Calculation Table

<table>
<thead>
<tr>
<th>Likelihood of Occurrence</th>
<th>Impact Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Low</td>
<td>Low</td>
</tr>
<tr>
<td>High</td>
<td>Very Low</td>
</tr>
<tr>
<td>Moderate</td>
<td>Very Low</td>
</tr>
<tr>
<td>Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>Very Low</td>
<td>Very Low</td>
</tr>
</tbody>
</table>

### Example Overall Risk Assessment Table

<table>
<thead>
<tr>
<th>Threat Event</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of Confidentiality</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Loss of Integrity</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>Loss of Availability</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Overall Risk Assessment Score</strong></td>
<td>Moderate</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authored by:</td>
<td>Richard Haugerud</td>
<td>IT CISO</td>
</tr>
<tr>
<td>Approved by:</td>
<td>Bret Blackman</td>
<td>IT CIO</td>
</tr>
</tbody>
</table>

Revision history of this Standard:

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>08/08/2022</td>
<td>Initial Standard Published</td>
</tr>
</tbody>
</table>