Exception Policy (ISP-15)

Document Owner

Executive Owner:	Darrell Morrison
Functional Area:	Information Technology

Authorization

Authorized By:	David J. Hinson
Position:	Interim Chief Information Officer
Signature	
Authorization Date	02/25/2025

Version History

Issue	Reason For Change	Date
1.0	Initial Release	02/25/2025

Review Period

Information Security Policies are to be reviewed at a minimum annually.

Change Control

Requests for changes to Information Security Policies are to be sent to the document owner providing details of the requested changes and a short justification.

Exceptions

Requests for exceptions to this policy are to be submitted in accordance with the exception policy. Note that all exceptions are time limited to no more than 12 months in duration.

Applicability

This policy applies to all faculty, staff and contractors issued access to University IT resources and services.

Table of Contents

Introduction

During the lifecycle of university services there will be cases where compliance with Policies and Standards cannot be achieved. An exception process allows the University to assess the risk of such cases and manage the risk in an ongoing and transparent manner.

Objective

This policy defines the process for submitting approving, recording, and managing the risk of any variations from policy and standards. For the exception policy to be effective, it must operate in a consistent, neutral, and timely fashion and not expose the organization to material risk.

Policy Statement

General

1. An exception shall be permitted if there is a legitimate business need to use the non-compliant service or configuration and there are compensating measures in place that ensure the overall security stance is not materially compromised.
2. Exceptions may only be granted by the CIO, CISO, or Qualified Individual.
3. All exceptions require a security risk review or assessment.
4. Exceptions are to be resubmitted for review at least annually.
5. If a certain type of exception is constantly being requested or approved, it may mean the relevant standard needs to be adjusted to include the exception as a norm.

Reasons for Requesting an Exception

1. A team or product is unable to meet policy and standards immediately but has improvements in the roadmap to do so. (Note that failure to plan is not an acceptable reason for exception approval)
2. An issue reported by the vulnerability scanning tool or similar may not apply to a specific service or delivery element and is in effect a false positive.
3. An alternate method for meeting compliance is available that offers equivalent or better security.

Process for Requesting an Exception

4. Requests for exception should be sought in exceptional cases and only where mitigation is excessively expensive, at odds with business operation or technically not feasible. The individual manager should assess the risk posed by the exception and identify mitigating measures to reduce that risk exposure.
5. The manager must complete the risk exception request form at Appendix 1 and review with the Director of Information Technology before passing it to the CIO or CISO for review.
6. The CIO or CISO should review the requests and assess the level of risk to the department and customer base prior to approving or rejecting the exception request.
7. The Director of Information Technology is to ensure all exceptions are also included in the central risk registry and the impact on overall risk stance modelled.
8. All active exceptions are to be logged centrally onto the shared drive and reviewed at least annually.

Appendix – 1 Exception Request Form

Instructions: complete all sections in light brown and delete all italic text. Note the maximum duration of any exception shall be 12 months.

Exception Name	*Simple Name*
Description of Exception	
Hosts or Devices	*Insert asset or unique CI names here*
Application or Service	
Submitter (Name)	
Risk Owner (Name	
Date Submitted	
Risk Assessment = Impact* Prob	
Impact (3 =high, 2 = med, 1 = low)	
Probability (3 =high, 2 = med, 1 = low)	
Reason for Non-Remediation	
Mitigation Measures Proposed	*Provide description of mitigation measures and status of those measures i.e., in progress or completed*
Risk Assessment Post Mitigation = Impact* Prob	
Impact (3 =high, 2 = med, 1 = low)	
Probability (3 =high, 2 = med, 1 = low)	
Exception Status	*Pending/Accepted/Rejected/Expired*
Risk Acceptor (VP or Director)	*Insert Name*
Date of Acceptance	
Date of Next Review	