



ITS Process: Exceptions Process

Author(s): Matthew Kunkel & Keela Ruppenthal

Date: June 1, 2016

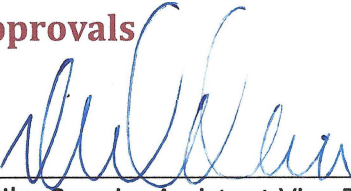
Version:



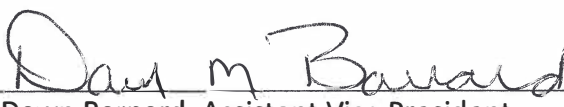
Revision History

Version No.	Date	Description	Author
1.0	June 1, 2016	Initial Release	Keela Ruppenthall

Approvals


 Mike Corwin, Assistant Vice President 6/3/16
Date


 Tom Ambrosi, Senior Director and Chief Information Security Officer 6/3/2016
Date


 Dawn Barnard, Assistant Vice President 6/3/2016
Date


 Tony Opheim, Associate Vice President and Deputy CIO 6/3/16
Date


 Dr. Sasi Pillay, Chief Information Officer 6/3/16
Date



Contents

Revision History	ii
Approvals	ii
1. Introduction	1
2. Purpose	1
3. Scope.....	1
4. External Requirements/Drivers	1
5. Effective Dates	2
6. Roles, Responsibilities, Accountabilities, and Authorities.....	2
Chief Information Officer or Delegate	2
Policy, Process, Procedure, or Standard Owner or Delegate	2
Subject Matter Expert.....	2
Requester	3
Requestor’s Manager/Supervisor	3
7. Policy.....	3
7.1. Criteria.....	3
7.2. Revocation.....	4
8. Process	4
8.1. Complete Exception Request Form.....	4
8.2. Supervisor/Manager Review and Approval	4
8.3. Subject Matter Expert Review	4
8.4. Policy, Process, Procedure, or Standard Owner Review and Approval	5
8.4.1. When there is no CIO appeal or approval step.....	5
8.4.2. When CIO approval is required.....	5
8.4.3. When an appeal is available	5
8.5. CIO Review and Approval (Where Required).....	5
8.6. Implementation.....	5
8.7. Renewals	6
9. Review Cycle	6
Appendix A: Glossary	7
Acronyms	7
Terms	7



Appendix B: Exceptions Request Form 8



1. Introduction

Washington State University (WSU) Information Technology Services (ITS) policies, procedures, processes, and standards individually and collectively institute controls that protect the business value of WSU Information Resources and ITS services. While every exception to a policy, procedure, process, or standard increases risk to Information Resources and services or represents an increase in administrative cost, occasionally scenarios exist where the value gained through an exception outweighs the cost and risk.

2. Purpose

All Information Resources that process, store, or transmit University data are expected to comply with all applicable policies, procedures, processes, and standards. Information Resource owners, who are accountable for ensuring appropriate enforcement of University policies, procedures, processes, and standards for WSU Information Resources, must follow this process in order to request an exception to those policies, procedures, processes, and standards.

In such cases, the exception must be documented and approved in full accordance with this process before it is considered a valid exception.

3. Scope

This process applies to all published policies, procedures, processes, and standards applicable to WSU Information Resources to which ITS has the authority to grant exceptions, to all Information Resources and services that are owned or managed by ITS, and to all ITS staff.

4. External Requirements/Drivers

List the Federal and/or State laws and regulations and/or Management Framework references that will be addressed by this document.

WSU is required to comply with Federal and/or State laws and regulations related to information security, privacy and data confidentiality. This policy complies with regulations as defined by:

- FERPA
- HIPAA
- GLBA
- Washington State OCIO Policy 141 – Securing Information Technology Assets

This Policy satisfies part or all of the following controls from NIST Special Publication 800-53 rev. 4:

- CA-1
- PL-1



- PL-2

5. Effective Dates

This process is effective immediately upon final approval.

6. Roles, Responsibilities, Accountabilities, and Authorities

Chief Information Officer or Delegate

- Determines which policies, processes, procedures, and standards are subject to the appeals process with respect to exception requests.
- Reviews and approves or denies appeals to denied exceptions.
- Determines if additional reviews are required to support the appeal.
- Determines if blanket exceptions are appropriate and communicates same to the campus.
- May revoke exceptions in the event an incident or violation occurs.
- Authorizes the exception process and recommends changes as needed.

Policy, Process, Procedure, or Standard Owner or Delegate

By default, this role is filled by the ITS senior leader (CIO direct report) for the ITS group which created and/or stewards the policy, process, procedure, or standard to which an exception is requested. That ITS senior leader may delegate the exception approval authority for individual policies, processes, procedures, or standards to another management role within ITS; however, the default ITS senior leader retains accountability for such exceptions.

- Reviews and approves or denies exception requests.
- Determines if additional reviews are required to support the request.
- Authorizes specific standardized conditions or requirements for granting an exception.
- Tracks requests for exception and reviews at least annually.
- Maintains exceptions documentation on the WSU ITS SharePoint website.
- May revoke exceptions in the event an incident or violation occurs.
- Accepts accountability for the business risks associated with granting each exception.

Subject Matter Expert

This role is assigned for each policy, process, procedure, or standard by the policy, process, procedure, or standard owner. Multiple subject matter experts may be assigned for the same policy, process, procedure, or standard.

- Reviews and aids in risk analysis for exception requests.
- Aids in performing additional reviews as directed by the policy, process, procedure, or standard to support the request.
- Recommends specific standardized conditions or requirements for granting an exception.



- Recommends possible compensating controls.

Requester

- Completes the exception request form in consultation with the subject matter expert and/or the policy, process, procedure, or standard owner.
- Ensures that the information provided in support of an exception request is accurate.
- Implements all compensating controls required as a condition of exception approval.
- Removes any implementation of an approved exception that has been revoked due to the occurrence of an incident or violation.
- Resubmits exception request for renewal as needed upon expiration.

Requestor's Manager/Supervisor

- Reviews and approves requests for exception involving staff under their management.
- Reviews applicable policy or standard for which the exception is being requested.
- Ensures that the information provided in support of an exception request is accurate.
- Ensures implementation of all compensating controls required as a condition of exception approval.
- Ensures removal of any implementation of an approved exception that has been revoked due to the occurrence of an incident or violation.
- Accepts managerial/supervisory accountability for the risks associated with granting the exception for their staff member(s).

7. Policy

7.1. Criteria

An exception to a published ITS policy, process, procedure, or standard may only be granted when one or more of the following criteria are met:

- The exception is temporary in duration, less than 90 days, and immediate compliance would disrupt critical operations.
- Another acceptable solution is proposed that provides equivalent risk levels or better.
- The exception is for a legacy system that is firmly scheduled for retirement and compliance is either not possible or not cost-effective in the interim.
- Compliance would adversely impact a specific University business process or processes on an ongoing basis to a degree that would not be offset by the reduced risk and/or increased efficiency occasioned by compliance
- Compliance for a specific case would cause an adverse financial impact that would not be offset by the reduced risk and/or increased efficiency occasioned by compliance

And all of the following criteria are met:

- Exceptions that create additional risk to the university above the minimal risk level without compensating controls will not be approved.



7.2. Revocation

Requests for exception may be revoked in the event of a security incident or a policy violation with respect to approved compensating controls or other relevant defense-in-depth controls.

8. Process

8.1. Complete Exception Request Form

Requester completes the Exceptions Request Form in Appendix B and forwards the completed form to their manager/supervisor for review and approval.

Prior to submission of the exception request to the policy, process, procedure, or standard owner, the request must document:

- The specific policy, process, procedure, or standard for which an exception is being requested
- The specific device(s), information system(s), users(s)/accounts(s) and/or service(s) for which the exception is being requested
- Data classification of associated device(s), information system(s), user(s)/accounts(s), and/or service(s)
- The nature of the exception, i.e., specific deviation from the policy, process, procedure, or standard
- Why an exception is required, e.g., what business need or situation exists, what alternatives were considered, and why are they not appropriate
- A risk analysis that includes an identification of the threats and vulnerabilities, how likely each is to occur, the potential costs of an occurrence, and the cost to comply.
- Plan for managing or mitigating those risks, e.g. compensating controls, alternative approaches
- Anticipated length of exception (The full anticipated duration should be indicated, even though approvals will only be granted for up to one year at a time.)
- Additional information as needed, including any specific conditions or requirements for approval

8.2. Supervisor/Manager Review and Approval

The requester's manager/supervisor must review the overall context of the exception request, to include risks that non-compliance causes for WSU Information Resources and business processes. If the manager/supervisor believes the risk/reward trade-off is acceptable, then the manager approves the exception request and forwards it to the applicable Policy, Process, Procedure, or Standard SME.

8.3. Subject Matter Expert Review

The SME assigned for the policy, process, procedure, or standard referenced in the exception will:

1. Review the request, contacting the requester if additional information is required.



2. Determine if other technical SMEs need to be consulted and contact them as needed
3. Update the request as needed based on the outcome of the review
4. If there are no significant changes, forward to the policy, process, procedure, or standard owner (or delegate) with a recommendation to approve or deny the request.
5. If there are significant changes to the original request, forward it back to the requester to review and re-sign if they concur with the changes. If the requestor does not concur with the changes, they may forward both versions to the policy, process, procedure, or standard owner (or delegate), indicating the specific changes to which they object.

8.4. Policy, Process, Procedure, or Standard Owner Review and Approval

The policy, process, procedure, or standard owner (or delegate), will review and approve or deny the request for an exception and notify the requester, requestor's manager/supervisor, and the SME in writing as to the approval or provide a written explanation of the denial.

8.4.1. When there is no CIO appeal or approval step

For approved exceptions to policies, processes, procedures, and standards not requiring CIO approval or for denials not eligible for an appeal to the CIO, the outcome is recorded in the exceptions system of record.

8.4.2. When CIO approval is required

For exceptions approved by the policy, process, procedure, or standard owner that require CIO approval, the policy, process, procedure, or standard owner forwards the exception request to the CIO.

8.4.3. When an appeal is available

Some policies, processes, procedures, and standards allow exception denials by their owner to be appealed to the CIO. At the discretion of the requestor and/or their manager/supervisor, a request for appeal is forwarded by the requestor's manager/supervisor up their management chain of authority to the CIO, with each successive level management reviewing and approving or denying the appeal request prior to the appeal reaching the CIO.

8.5. CIO Review and Approval (Where Required)

The Information Services Chief Information Officer or designee, will approve or deny the request for an exception or appeal and notify the requester, requestor's manager/supervisor, SME, and the policy, process, procedure, or standard owner in writing as to the approval or provide a written explanation of the denial. The outcome is recorded in the exceptions system of record.

8.6. Implementation

If the exception requires implementation, those implementations must be performed in accordance with normal change policies and processes. Where the relevant technology allows, any changes implemented should have a note added to indicate the current expiration date of the exception.



8.7. Renewals

Unless otherwise specified, exceptions will be valid for one year. Due to the continually changing information environment, exceptions will not be granted for more than one year at a time. It is the responsibility of the requestor and their manager/supervisor to ensure that exceptions are renewed by re-initiating this process. The prior year's request form may be reused so long it is updated to reflect any changes.

9. Review Cycle

This process will be reviewed at least annually and updated as needed.



Appendix A: Glossary

Acronyms

Acronym	Definition
IT	Information Technology
ITS	Information Technology Services
NIST	National Institute of Standards and Technology
WSU	Washington State University

Terms

Term	Definition



Appendix B: Exception Request Form

ITS Exception Request Form

Requestor	
Requested Start Date	
Requested Expiration Date (Not to exceed one year from the start date of the exception.)	
Policy, process, procedure, or standard for which an exception is being requested	
Policy, process, procedure, or standard owner	
Specific device(s), information system(s), users(s)/accounts(s) and/or service(s) for which the exception is being requested	
Data Classification of associated device(s), information system(s), user(s)/accounts(s), and/or service(s)	
Nature of the exception requested (Describe the specific deviation from the policy, process, procedure, or standard.)	
Justification for the Exception (What business need or situation exists that causes compliance to be infeasible? What increase in value would the exception provide?)	
Costs What would be the cost of compliance without the exception? What would be the cost of implementing the exception?	



<p>Alternatives</p> <p>What alternatives to an exception were considered, and why were they infeasible?</p>	
<p>Threats and Vulnerabilities</p> <p>What threats and vulnerabilities are relevant to the exception, and how does the exception alter WSU's exposure to them?</p>	
<p>Risk Level</p> <p>Based on the above and the potential impact of a compromise to the affected resources, what is the risk presented by the exception?</p>	
<p>Compensating Controls</p> <p>What is the plan for managing or mitigating those risks, e.g. compensating controls, alternative approaches</p>	
<p>Anticipated Overall Length of Exception (The full anticipated duration should be indicated, even though approvals will only be granted for up to one year at a time.)</p>	
<p>Basis for Approval/Denial of Exception Request</p>	
<p>Additional information as needed, including any specific conditions or requirements for approval</p>	

Reviews, Approvals, and Acceptances

Requestor's Manager/Supervisor Approval _____ Date

Subject Matter Expert Review _____ Date



Policy, Process, Procedure, or Standard Owner (Or Delegate) Approval Date

CIO Approval (As Required) Date

Requestor Acceptance Date