Exception Policy

Statement of Policy
Washington University in St. Louis (WashU) is committed to conducting all university activities in compliance with all applicable laws, regulations, and university policies. WashU has adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use.

Objective
The policy and associated guidance provide a well-defined approach to review exception requests for published WashU Information Security policies, standards, and guidelines.

Applicability
This policy is applicable for WashU infrastructure, network segments, and systems.

Audience
The audience for this policy is all WashU faculty, staff, and students. It also applies for all other agents of the university with access to WashU information and network for contracted services. This includes, but not limited to partners, affiliates, contractors, temporary employees, trainees, guests, and volunteers. The titles will be referred collectively hereafter as “WashU community”.

Roles & Responsibilities

Policy
WashU Information Security policies, standards, and guidelines are developed based on regulatory, state, federal, and industry requirements. They also use NIST and Office of Information Security (OIS) guidance to ensure confidentiality, integrity, and availability for systems and information. WashU recognizes objectives and technology needs for the departments and schools may be impacted by compliance requirements.

The department or school that is not able to meet the policies and standards will submit a policy exception request form to explain why compliance is not possible, systems(s) that will be impacted, information and system classification, end users, impact, duration for the exception, suggestions of compensating controls that may be applied, and the plan the department or
school has to meet the compliance requirements. Completion of the form may require assistance from the supporting IT department, data owner, and system owner.

Exception requests will be reviewed on a case-by-case basis to identify the risk for impact to the university; not every exception may be able to be approved and implemented. Requests for an exception for convenience will not be approved.

Upon receipt of the completed form, diagrams, and reference material for the request, OIS will perform a risk assessment. Final assessment reports are returned within two to three weeks. If this timeline will not be achieved, OIS will provide an updated timeline.

Exceptions which are assigned a high risk for the university will be escalated to the CISO for review. The CISO may request additional information from the department or school.

Until approval has been granted the requested exception will not be implemented.

Exceptions will be tracked and reviewed at a minimum annually.

Exception status may change at any time due to an incident or significant risk to WashU information, network, or systems.

**Policy Compliance**
The OIS will measure the compliance to this policy through various methods, including, but not limited to – reports, internal/external audits, and feedback to the policy owner. Exceptions to the policy must be approved by the OIS in advance. Non-compliance will be addressed with management, Area Specific Compliance Office, Human Resources, or the Office of Student Conduct.

**Related Policies**
None

**Reference**
Policy Exception Process
Policy Exception Form

**Policy Review**
This policy will be reviewed at a minimum every three years.

**Title:** Policy Exception Policy  
**Version Number:** 1.0  
**Reference Number:** PL-01.07  
**Creation Date:** February 7, 2019  
**Approved By:** Security and Privacy Governance Committee  
**Approval Date:** May 15, 2019
Status: Final
Scheduled Review Date: June 1, 2022
Revision Date:
Revision Approval Date:
Policy Owner: Office of Information Security