Information Security Controls 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 and organized approach for compliance with identified security controls.

Applicability
This policy is applicable to all WashU systems and network segments.

Audience
The audience for this policy is IT users with elevated permissions.

WashU faculty, staff and students will need to be aware of this policy. This 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 executive management and governance boards require all personnel, departments, and schools to ensure sensitive information used and held by the University is protected to assure the confidentiality, integrity and availability.

The Information Security Office (ISO) will review and identify the applicable security frameworks – International Organization for Standardization, National Institute of Standards and Technology (NIST) Security Controls (SP800-53) and other identified industry standards to be applied within WashU departments and schools. Controls will be assigned to create protection levels within the infrastructure commensurate with risk. Control assignments will be
based on the information classification – (protected, confidential and public) and system classification (regulated, business, research, academic) of the information created, hosted or transmitted within the infrastructure.

The ISO will identify the controls the departments and schools will need to implement, develop process, and document for compliance.

**Policy Compliance**
The ISO 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 ISO in advance. Non-compliance will be addressed with management, Area Specific Compliance Office, Human Resources or the Office of Student Conduct.

**Related Policies**
Information Classification Policy

**Reference**
https://www.nist.gov/
System Classification Standard
Control Zone Standards

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

**Title:** Information Security Controls Policy  
**Version Number:** 1.0  
**Reference Number:** PL-01.05  
**Creation Date:** March 6, 2018  
**Approved By:** Security and Privacy Governance Committee  
**Approval Date:** June 1, 2018  
**Status:** Final  
**Scheduled Review Date:** March 1, 2022  
**Revision Date:** February 26, 2019  
**Revision Approval Date:** March 15, 2019  
**Policy Owner:** Information Security Office