Infrastructure Security 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 the WashU computing community directives to help ensure integrity, confidentiality, and availability of information and provide a safe computing environment. All network assets, systems, computing devices, services, and operating personnel will be in scope for this policy. This includes network infrastructure components, network management and service systems, WashU faculty, staff and students.

Applicability
This policy is applicable to all infrastructure connected to the WashU 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
The infrastructure shall, with exceptions noted and approved by the Information Security Office (ISO) and IT leadership, will follow the WashU IT and Information Security Policies, Standards and Guidelines described in https://informationsecurity.wustl.edu. Controls will be adapted from Special Publications of the National Institute of Standards and Technology (NIST) SP800 series and other applicable standards.
The infrastructure will be designed to ensure the confidentiality, integrity, and availability (CIA) of information. In particular, the protection of systems and information against unauthorized access, against unauthorized modification or disclosure, and protection of systems against denial of service. The degree of protections applied within parts of the infrastructure will be commensurate with bringing risks to acceptable levels.

Components or systems connected to the WashU infrastructure used to store, transmit or process confidential and/or protected information will be setup to protect the data being stored, accessed or transmitted.

Responsibility for designing, implementing, and maintaining security protections resides with the information technology staff, director or department heads will retain responsibility for ensuring compliance with this policy. In addition to management and information technology staff, the individual user is responsible for the information technology equipment and resources under their control.

To protect the integrity of the infrastructure and mitigate the risks and losses associated with external and internal threats WashU will:

- Design the Infrastructure to ensure appropriate security controls are in place commensurate with data classification levels, business criticality and in compliance with state and federal regulations.
- Ensure applicable federal regulations, organizational policies, and mandates to protect information are taken into consideration within the infrastructure.
- Recommend effective security controls based on risks and a cost benefit assessment which meet the intent of applicable regulations and university policies.
- Create accountability within the network and other computing resources in which individuals have access.
- Give and assist network managers, engineers, and technicians guidance in the implementation of controls in addition to maintaining and operating the infrastructure in a secure manner.
- Ensure that all critical functions of infrastructure are documented, have operational processes, and disaster recovery plans to provide continuity of operation.
- Maintain Confidentiality, Integrity, and Availability (CIA) of the information at WashU.
- Follow established standards for all infrastructure components (physical or virtual) containing WashU information.

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
None

Reference
None

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

Title: Infrastructure Security Policy
Version Number: 3.0
Reference Number: PL-01.04
Creation Date: February 19, 2011
Approved By: Security and Privacy Governance Committee
Approval Date: July 5, 2016
Status: Final
Scheduled Review Date: March 1, 2022
Revision Date: February 26, 2019
Revision Approval Date: March 15, 2019
Policy Owner: Information Security Office