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

This policy and associated guidance are meant to provide the WashU computing community directives to help ensure integrity, confidentiality and availability of information and provide a safe computing environment.

Scope

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, and WashU faculty, staff and students.

Policy

The infrastructure shall, with exceptions noted and approved by the Information Security Office (ISO) and the CIO, will follow the WashU IT and Information Security Polices, 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 Wash U 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 his or her control.

To protect the integrity of the infrastructure and mitigate the risks and losses associated with external and internal threats the ISO will work with WashU departments and schools to:
- 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 and 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.

Title: Infrastructure Security Policy
Version Number: 2.0
Creation Date: February 19, 2011
Applicability: Protected, Confidential and Public
Reference Number: 03.02
Status: Final
Revision Date: July 5, 2016
Policy Owner: Information Security Office