Washington University in St. Louis

Office of Information Security
University Information Security Policies

Information 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 management direction and support for the information security program in accordance with university requirements, relevant laws, and regulations.

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

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
Information security is the protection of electronic information from threats in order to ensure business continuity, minimize risks, and maximize university opportunities.
The Office of Information Security (OIS) will manage the information security program at WashU. Information security is not the purview of any one functional group. Cooperation from all departments and schools is required to secure the environment and satisfy compliance requirements.

Training and awareness will be provided to ensure all workforce members and students know their security responsibilities. WashU community members are responsible for compliance, securing devices used to connect to the WashU network, the information they receive, store,

utilize, and transmit. OIS will provide training and awareness for WashU through in person training sessions or Learn@work courses, E-mail messages or alerts, digital signage, and the OIS website.

The OIS will engage directly with the departments and schools to support the mission of clinical, research, and academic excellence by ensuring the information system assets and data is protected at a level commensurate with their classification, sensitivity, and criticality of information.

The OIS will develop and maintain administrative, technical, and physical safeguards to protect confidentiality, integrity, and availability of the information systems assets, regulated, and confidential information.

The information system assets and data must be consistently and appropriately protected and classified regardless of their stage in the life cycle from origination to destruction.

Process documentation, policies, and logs will be maintained and reviewed by departments and schools to ensure:

- security requirements are being implemented
- accounts are created with least privileges
- separation of duties to reduce the risk of conflict of interest, fraud, and one person is not responsible for all phases or requirements of a process.

Workforce members managing contracts with vendors and third-parties for the university, school, or department or level to host, transmit, or process university protected and confidential information are responsible to ensure they will, at a minimum, meet WashU policies, standards, and guidelines.

The OIS will monitor and review the safeguard measures and controls implemented by departments and schools. Changes in the law, industry regulations, technology, WashU policies, standards, guidelines, and procedures will be reviewed and the necessary changes will be implemented.

An independent review of the information security program will be performed at a minimum every three years.

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
None

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

Title: Information Security Policy
Version Number: 3.0
Reference Number: PL-01.02
Creation Date: November 15, 2007
Approved By: Security and Privacy Governance Committee
Approval Date: April 6, 2016
Status: Final
Scheduled Review Date: March 1, 2022
Revision Date: February 26, 2019
Revision Approval Date: March 15, 2019
Policy Owner: Office of Information Security