

Statement of Policy

Washington University in St. Louis (WashU) is committed to conducting 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

Establish a common methodology and organized approach to Information Security risk management whether based on regulatory compliance requirement or a threat to the university.

Scope

The information security risk management process covers all administrative, physical, technical process that enable and govern protected and confidential electronic information whether created, stored (on site or externally hosted), processed or transmitted by WashU faculty, staff, students and supporting infrastructure.

Risk Governance

Leadership shall steer the institution towards actions that ensure cyber risk taking activities are aligned with the institution's capacity to withstand losses and its missions of education, research and healthcare. It will create a balance between the risk presented to the university and its ability to conduct its operations.

Policy

WashU Information Security Office recognizes the university is continually exposed to internal and external risks. WashU Information Security office (ISO) is committed to an ongoing risk management process to protect WashU information, assets and its ability to perform its mission.

The ISO will develop and maintain an Information Security Risk Management Process to frame, assess, respond and monitor risk. Guidance for this process will be based on the International Organization for Standardization, ISO27001, ISO27005, ISO31000 frameworks and specific security regulations e.g. HIPAA, PCI-DSS, FERPA, etc. The risk management process will be designed to assist WashU maintain compliance with regulatory requirements, federal and state and local laws. Refer to the Information Security Risk Management Process for instructions.

Risk management will involve the entire WashU community. The ISO will engage with our stakeholders, workforce members, departments and schools to increase awareness and communication of risk and to identify methods to integrate risk management in university culture, events, projects, processes, strategic and operational planning. Expectations for all workforce members will be open, clear and transparent.

The ISO will identify, categorize, prioritize and report risks based on the probability and potential impact to the environment if confidentiality, availability and / or integrity is compromised. The risk evaluation will be uniform and consistent for WashU departments and schools. Dependencies for departments and school will also be included in the risk evaluation.

Risk Register

The Risk Register is currently comprised of a series of unrelated spreadsheets across a combination of administrative and academic units and risk types.

The CISO is responsible for maintaining the risk register.

The purpose of the Risk Register is to consolidate all information about risk is into a central repository. This allows risk management participants to use a single resource to obtain the status of the risk management process.

The risk register shall comprise the following minimum components:

Date:	The date that risks are identified or modified. Optional dates to include are the target and completion dates.
Risk Number:	A unique identifying number for the risk
Assessment ID:	Unique Identifier from risk assessment reports that identified the risk
Risk Description:	A brief description of the risk, its causes and its impact
Existing Controls:	A brief description of the controls that are currently in place for the risk
Consequence:	The consequence (severity or impact) for the risk
Risk Ranking:	A priority list which is determined by the relative ranking of the risks by their qualitative risk score
Risk Mitigation Strategy:	The action which is to be taken to reduce the risk
Risk Owner:	The person who has the responsibility for the risk, manages the risk mitigation efforts and the risk response if the risk occurs

Roles and Responsibilities

Roles	Responsibilities
Board of Directors Audit Committee	<ul style="list-style-type: none">• Presented annual risk update
Executive Leadership	<ul style="list-style-type: none">• Approves Capital Expenditures for Information Security• Communication Path to Deans and Senior Faculty
CIO	<ul style="list-style-type: none">• Sponsors the ISO to ensure the information security risk process is followed for university activities, processes and projects

CISO	<ul style="list-style-type: none"> • Will maintain the risk register • Communicate information security risks to Executive Leadership • Will report annually to university leadership on risks that need to be addressed to bring risk to acceptable level
Information Security Office	<ul style="list-style-type: none"> • Responsible for conducting risk assessments, documenting the identified threats and the likelihood of occurrence. • Develop policy, procedure and solutions to mitigate identified risk to an acceptable level.
Internal Audit	<ul style="list-style-type: none"> • Conduct sample audits to ensure compliance to information security policies and risk mitigation efforts
School & Departmental Stakeholders	<ul style="list-style-type: none"> • Responsible for the implementation of risk mitigating controls and ensure they are properly maintained
Employees	<ul style="list-style-type: none"> • Acting at all times in a manner which does not place at risk the health and safety of themselves, other person in the workplace, and the information and resources they have use of • Helping to identify areas where risk management practices should be adopted • Taking all practical steps to minimize the University's exposure to contractual and regulatory liability.

Reporting

The ISO will use a risk log or register to assist with documenting the identified risks and their status.

The Chief Information Security Officer (CISO) will deliver a risk management report annually to the Board of Director Audit Committee. The report will provide a view of the strategic and operational risks identified and any steps taken to mitigate the risk.

Response

The appropriate university response will be based upon identified risk tolerance levels – remediate, mitigate, transfer, accept or avoid. Plans will be developed and response to the risk will be assigned to the department or school to take the steps to reduce risk to an acceptable level. Cooperation from all schools and departments will be required to reduce risk in the WashU environment. These steps will be monitored, tracked in the risk register, tested and reported to senior leadership.

Risk Management Performance

Performance will be identified and measured by

- The reduction or risks reported quarterly
- Completion and reporting of reviews
- Compliance with regulation
- Information Security incidents that are investigated and analyzed for risk resulting in the appropriate response or controls implemented
- Risk assessments completed for all university events and projects

Policy Review

Risk management will be an ongoing process. The risk management policy and process will be reviewed annually and if necessitated by regulatory or legislative changes.

Related Documents

Risk Management Plan
Risk Assessment Process

Title: Information Security Risk Management Policy

Version Number: 2.0

Creation Date: November 27, 2007

Applicability: Protected and Confidential

Reference Number: 01.03

Status: Final

Revision Date: December 6, 2016

Policy Owner: Information Security Office