Washington University in St. Louis

Office of Information Security
University Information Security Policies

Roles and Responsibilities

Statement of Policy
Washington University in St. Louis (WashU) is committed to conducting business 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 establish the roles and responsibilities within WashU, which is critical for effective communication of information security policies and standards. Roles are required within the organization to provide clearly defined responsibilities and an understanding of how the protection of information is to be accomplished. Their purpose is to clarify, coordinate activity, and actions necessary to disseminate security policy, standards, and implementation.

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

Audience
The audience for this policy includes all WashU faculty, staff, and students who are involved with the Information Security Program.

Awareness of this policy 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

The following Roles are defined.

Roles	Responsibilities
Board of Directors Audit Committee	• Presented annual IT state and risk update • Consults with Executive Leadership to understand University IT mission and risks and

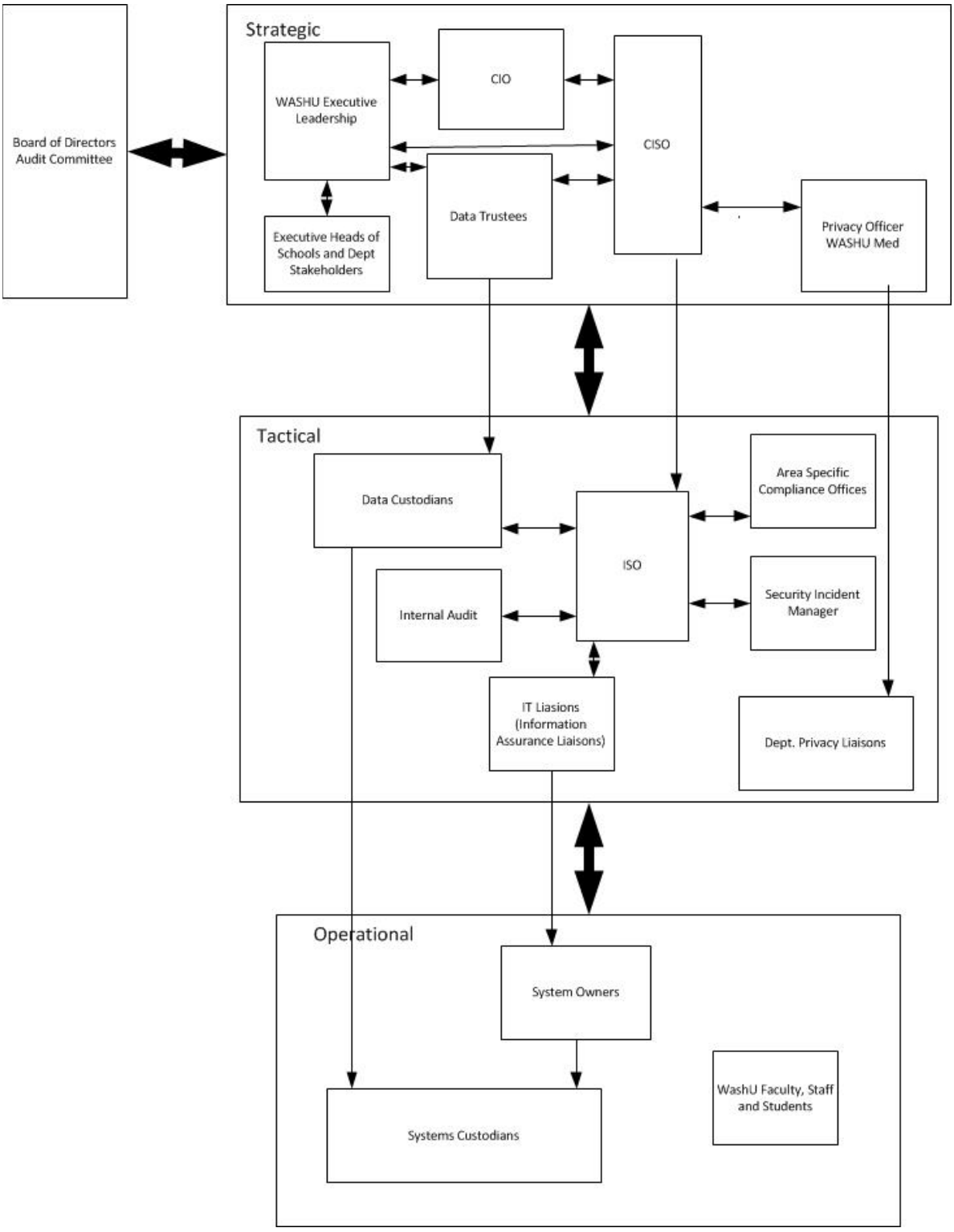
	provides guidance to bring them into alignment
Executive Leadership	• Approves Capital Expenditures for Information Security • Communication Path to Deans and Senior Faculty • Aligns Information Security Policy and Posture based on the University's mission and risks
CIO	• Sponsors the Office of Information Security (OIS) to ensure the information security risk process is followed for university activities, processes, and projects • Coordinates with the CISO to ensure IT puts into practice the Information Security Framework
CISO	• Communicates information security risks to executive leadership • Reports information security risks annually to university leadership and gains approval to bring risks to acceptable levels • Coordinates the development and maintenance of information security policies and standards • Works with the OIS to establish an information security framework and awareness program • Serve as liaison to the Board of Directors, Law Enforcement, Internal Audit, and General Council
Data Trustees	• Has oversight responsibility for information related to the university's mission that is managed, administered, or run by the depts. and schools • Authorizes/Defines policies, standards, and guidelines regarding business definitions of information, access, and usage of that information • Appoints a data custodian(s) for their subject area • In some cases, responsible for the context, content, and associated business rules and use. (Typically delegated to the data steward)
Privacy Officer WASHU Med	• Provides oversight and direction for privacy within the healthcare environment to include incident investigations and determination of notification requirements involving protected health information (PHI) • Work closely with senior administrators and compliance staff to enforce HIPAA privacy program policies within the medical school
Area Specific Compliance Offices (ASCO's)	• Responsible for their specific privacy compliance areas • Works with the OIS to ensure any information security requirements are met
Office of Information Security (OIS)	• Responsible for conducting risk assessments, documenting the identified threats, and maintaining risk register • Assist WashU departments and schools in assessing their data for classification as defined in the Information Classification Policy and advises them of required controls

	• Develop policy, standards, process, and solutions to mitigate identified risk to an acceptable level • Assists the CISO with the development of the Information Security Framework • Works with IT, faculty, and staff to embed the framework into operations • Monitors the infrastructure and data repositories for malicious activity • Works with the incident manager in the investigation of security incidents • Responsible for establishing the Vulnerability Management program • Provide consulting services for information security throughout the university
Internal Audit	• Conduct sample audits to ensure compliance to information security policies and risk mitigation efforts • Interfaces with external auditors to provide independent audit of IT infrastructure and practices
Data Custodians	• Implement and enforces University policies, standards, and guidelines for institutional information within their designated data sets • Accountable for the security, privacy, data definitions, data quality, and compliance to data management policies and standards for a specific data domain • Has the primary responsibility for the accuracy, privacy, and security of a designated data set • Ensures access to the data is authorized and controlled; technical processes sustain data integrity and technical controls safeguard data • Works with the System Custodian to ensures that information which has been classified as confidential or protected adheres to University Information Security controls
Security Incident Manager	• Under the direction of the OIS, manage and coordinate incident response, communication, and notification • Serves as a lead in the investigation of security incidents • Coordinates and maintains incident documentation and documentation retention activities.
Dept. IT Liaisons	• Serve as a point of technical contact for the university information security committees and as an official for the organizational area(s) for which they are responsible in matters related to information security • Communicate with and educate workforce members in IT regarding the confidentiality, integrity, and availability of institutional information, information systems, and relevant university information security policies, standards, and guidelines for their organizational area(s) for which they are responsible • Facilitate requests for access to information systems upon request by the data custodians, system owners, and managers by obtaining proper approval and determining appropriate access needs for staff • Facilitate resolution of information security and privacy issues for the organizational area(s) for which they are responsible

	• Serve as focal point and coordinator during a security incident
Dept. Privacy Liaisons	• Act as the department or school's central contact regarding information security • Attend and participate in periodic privacy meetings, seminars, and retreats • Propagate new information, policies, and procedures to the appropriate school or departmental heads, division leaders, staff, Business Manager, etc. • Work with IT liaisons to manage and track a detailed inventory of the department's protected information • Provide input and feedback to the OIS regarding policy making, procedures, exceptions, and other department or school's issues pertaining to Information Security • Manage the implementation of compliancy rules and safeguards according to the policies and procedures • Coordinate Information Security training effort within the department or school • Serve as focal point and coordinator during a security incident
System Owners	• Manage the confidentiality, integrity, and availability of the information systems for which they are responsible. This shall include developing and implementing a process for managing access to information systems for which they are responsible, and other processes or controls in compliance with university policies on information security and privacy • Advise executive leadership on the financial resources necessary to develop and implement information systems and controls, including those specifically required by grants or contracts • Maintain critical information system documentation; and ensures and applies security controls per policies and standards • Formally appoint and delegate responsibility to system custodians
System Custodians	• Making and being accountable for operational decisions about the use and management of an information system • Responsibilities as delegated by system owners and data custodians for implementation of controls. • System Custodians may be the same as the owners
WashU Faculty, Staff and Students	• 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

Policy

The Roles and Responsibilities established above shall be established within WashU to ensure efficient dissemination of university Information Security policies and the protection of information.



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: Roles and Responsibilities Policy
Version Number: 1.0
Reference Number: PL-01.03
Creation Date: February 6, 2019
Approved By: Security and Privacy Governance Committee
Approval Date: March 15, 2019
Status: Final
Scheduled Review Date: March 1, 2022
Revision Date:
Revision Approval Date:
Policy Owner: Office of Information Security