Information Classification 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 identification and classification of information created, stored, and/or transmitted.

Applicability
This policy is applicable to all WashU information, infrastructure, 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 that is created, stored, or transmitted will be classified as public, confidential, or protected. The data owner will assist with data classification.

Faculty, staff, and students will assess the information prior to sharing with a third party to ensure sharing the information will not cause damage or distress. If there is potential for damage or distress, extra controls will be needed before the information is transferred.

Public
Information that is acceptable to share openly and does not have regulatory or industry requirements on its control and use is classified as public.
Confidential
Information that is not freely available to create, store, and transmit, but does not have any regulatory compliance, is confidential. This may include data provided to WashU by external individuals or entities for use or storage by the university.

Intellectual property of a department, school, research group, employee salaries, unlisted phone numbers, email address lists for studies or volunteers, human resource files, and legal documents would fall into this category.

This information is for limited distribution and requires basic information security controls.

Protected
Information identified by federal, state, local, and industry regulations is classified as protected. This information is regulated and requires information security controls in accordance to the mandates of those regulatory bodies.

Regulations including, but not limited to:
- Health Insurance Portability and Accountability (HIPAA) covering protected health information
- Federal Information Security Management Act (FISMA) when creating and storing information for federal agencies
- Payment Card Industry (PCI) Data Security Standards (DSS)
- Department of Homeland Security (DHS) covering controlled chemicals and substances
- Family Educational Rights and Privacy Act (FERPA)
- Chemical Facility Anti-Terrorism Standards
- FDA Part 11
- Nuclear Regulatory Commission (NRC)

Policy Compliance
The Office of Information Security (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
Encryption Policy

Reference
None
Policy Review
This policy will be reviewed at a minimum every three years.

Title: Information Classification Policy
Version Number: 3.0
Reference Number: RA-01.02
Creation Date: September 21, 2007
Approved By: Security and Privacy Governance Committee
Approval Date: April 6, 2016
Status: Final
Scheduled Review Date: March 1, 2016
Revision Date: February 26, 2019
Revision Approval Date: March 15, 2019
Policy Owner: Office of Information Security