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

Identify common classification of information that WashU uses, stores and/or transmits.

Policy

Information that is used, stored or transmitted will be classified as public, classified or protected. The data owner will assist with data classification and labeling.

Workforce members 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

Public information consists of information that is acceptable to share openly and has no requirements from federal or local regulations on its control and use.

Confidential

Information that is not freely available to use, 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 or 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 and local 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, storing information for federal agencies.
- Payment Card Industry (PCI) Data Security Standards (DSS)
- Department of Homeland Security (DHS) covering controlled chemicals and substances
- FERPA – Family Educational Rights and Privacy Act
- Chemical Facility Anti-Terrorism Standards
- FDA Part 11
- NRC – Nuclear Regulatory Commission

Title: Information Classification Policy
Version Number: 2.0
Creation Date: September 21, 2007
Applicability: Protected, Confidential and Public
Reference Number: 02.02
Status: Final
Revision Date: April 6, 2016
Policy Owner: Information Security Office