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

An Incident Response Policy is documented to provide a well-defined, organized approach for handling any potential threat to computers and data.

Policy

At WashU computer and network security incidents are processed by Information Security Office (ISO) in coordination with the department, Human Resources and/or General Counsel.

ISO should be notified of all computer and network security incidents that may affect the confidentiality, availability and/or integrity of the computer equipment or data at WashU. WashU departments and schools may use their own incident handling procedures to SUPPLEMENT this process under the direction of the Information Security Office.

- If the incident involves law enforcement or has legal ramifications it is important to preserve the scene, document the situation and not to destroy evidence that may reside within the system. There are Forensic processes that must be adhered to and it is highly recommended that the Information Security Office be involved and a trained Computer Forensics expert be used. May require outside experts to handle.
- ISO will notify the Area Specific Compliance Office (ASCO) for incidents that involve protected information.

Title: Incident Response Policy
Version Number: 2.0
Creation Date: September 18, 2009
Applicability: Protected, Confidential and Public
Reference Number: 02.01
Status: Final
Revision Date: May 19, 2016
Policy Owner: Information Security Office
Next Review Date: May 1, 2017