Incident Response 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 a well-defined and organized approach for handling any potential threat to computers and data.

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
At WashU, computer and network security incidents are processed by Information Security Office (ISO) in coordination with the department, WashU Protective Services, 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 information at WashU.

WashU departments and schools may use their own incident handling procedures to SUPPLEMENT this process under the direction of the ISO.
• 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 ISO be involved and a trained computer forensics expert be used or may require outside experts to handle.

• ISO will notify the Area Specific Compliance Office (ASCO) for incidents that involve protected information.

ISO will formalize a post incident response process and documentation of the lessons learned.

Policy Compliance
The ISO 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 ISO 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
Incident Management Process

Policy Review
This policy will be reviewed at a minimum every three years.

Title: Incident Response Policy
Version Number: 3.0
Reference Number: IR-01.02
Creation Date: September 18, 2009
Approved By: Security and Privacy Governance Committee
Approval Date: May 19, 2016
Status: Final
Scheduled Review Date: March 1, 2022
Revision Date: February 26, 2019
Revision Approval Date: March 15, 2019
Policy Owner: Information Security Office