Incident Reporting 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, organized approach for reporting any potential threat to confidentiality, availability and/or integrity of the computer equipment or information at WashU.

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
If you suspect a security incident has occurred, report it to your IT Service Desk or Security Liaison immediately. The Information Security Office (ISO) should also be notified of all computer and network security incidents. Security incidents have the potential to affect the confidentiality, availability and/or integrity of the computer equipment or data at WashU.

According to Community Emergency Response Team (CERT), a security incident can have the following definitions:

1. Violation of an explicit or implied security policy
2. Attempts to gain unauthorized access
3. Unwanted denial of resources
4. Unauthorized use of electronic resources
5. Modification without the owner’s knowledge, instruction, or consent
6. Theft or displaced University IT property or data
7. Malicious code

In addition to the initial report, complete and email the Incident Report Form to infosec@wustl.edu.

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
None

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

Title: Incident Reporting Policy
Version Number: 2.0
Reference Number: IR-01.01
Creation Date: November 19, 2015
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