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

To provide a well-defined, organized approach for reporting any potential threat to confidentiality, availability and/or integrity of the computer equipment or data at WashU.

Policy

If you suspect a security incident has occurred report it to your IT Help 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.

Title: Incident Reporting Policy
Version Number: 1.0
Creation Date: November 19, 2015
Applicability: Protected, Confidential and Public
Reference Number: 02.08
Status: Final
Policy Owner: Information Security Office