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 outline the physical and logical security controls needed to prevent unauthorized access or use and provide the availability and integrity of the environment.

Policy

Physical areas with servers, Storage Area Network (SAN), core networking and communication infrastructure other core support equipment, store and process protected information must have both logical and physical controls to prevent the unauthorized access and use of the information. Data centers will be reviewed periodically by Information Security and Internal Audit to validate that appropriate controls are in place.

Data Center Physical Security

- Locations will be secured to prevent unauthorized entry and must have locks that record access, cameras monitoring activity and environmental alarms to warn of threats to the computing environment.

Data Center Access Control

- Secure areas will be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
- Controls will be in place to log and monitor access to secure areas.
- Perform periodic reviews of logs and access permissions to validate that they are appropriate and approved.

Equipment Placing and Protection

- Equipment will be placed in protected areas to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
- All installations and removal of equipment will be formally documented and reviewed by facility care taker and/or IT management.

Environmental

- Centers that house mission critical services will have the appropriate cooling, fire suppression and redundant power services to maintain the environment in the case of an outage.

Cabling
• Power and telecommunications cabling carrying data or supporting information services will be protected from interception or damage.

Power Supplies

• Equipment will be protected from power failures and other electrical anomalies. A suitable electrical supply will be provided that conforms to the equipment manufacturer’s specifications.

Title: Data Center Policy
Version Number: 2.0
Creation Date: September 19, 2011
Applicability: Protected and Confidential
Reference Number: 03.01
Status: Final
Revision Date: April 6, 2016
Policy Owner: Information Security Office