Data Center 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 provides an outline of the physical and logical security controls needed to reduce the risk of unauthorized access or use of systems in a WashU data center.

Applicability
This policy is applicable to all WashU data centers.

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
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 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 they are appropriate and approved.

Data Center Delivery and Loading Areas
- Access to delivery and loading areas will be authorized, monitored, and controlled to ensure systems entering and leaving are documented.

Equipment Placing and Protection
- Equipment will be placed in protected areas to reduce the risks from environmental threats, 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 which conforms to the equipment manufacturer’s specifications.

Policy Compliance
The Information Security Office 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
Policy Review
This policy will be reviewed at a minimum every three years.

Title: Data Center Security Policy
Version Number: 3.0
Reference Number: PE-01.01
Creation Date: September 19, 2011
Approved By: Security and Privacy Governance Committee
Approval Date: April 6, 2016
Status: Final
Scheduled Review Date: March 1, 2022
Revision Date: February 26, 2019
Revision Approval Date: March 1, 2019
Policy Owner: Information Security Office