James Madison University Information Technology

Standard for Managing Physical and Environmental Security of IT Facilities

January 2024

Purpose:

This standard identifies the physical and environmental requirements for ensuring the security of areas that contain the University's sensitive data, whether managed by Information Technology (IT) or a department outside of IT. The goal of this standard is to ensure compliance with ISO 27002:2022 standards and other best practices for the physical and environmental aspects of information security.

Definitions:

IT Facility: A data center, server room, or other physical space that contains servers, storage area networks, data storage media, or any other device on which data is stored electronically. IT may, at its sole discretion, broaden the scope to include other areas such as telecom rooms that contain core network devices, service provider demarcations, or other mission critical equipment. Only central IT designates facilities as data centers and all such facilities are their responsibility.

Responsible party: The University department or team who is responsible for or operates a given IT Facility.

Standard:

1. Suitability and Singularity of Purpose

An IT Facility has no other use. It does not serve any additional functions such as office space, a workroom, or storage space for items other than those needed for its operation. It is a space that is capable of being physically secure, with minimal or no windows, minimal glass in doors, and little or no visibility from the outside.

2. Access Control and Intrusion Detection

All university IT Facilities are furnished with card access control. The Responsible Party establishes an approval process for card access to its facility and grants and revokes access with proper approvals. Individuals with access who leave the University or change roles have their access revoked or updated promptly, as appropriate and with proper approval. All access management activities are recorded and preserved for auditing purposes.

Data centers are furnished with intrusion alarms. The IT Systems and Operations team grants alarm codes for Data Centers along with approved card access. Codes for disarming and rearming the intrusion alarms are assigned to specific teams or groups that share a common need for access to an IT Facility. Whenever access is terminated for a group member, Systems and Operations will assign a new code to the entire group. Records of alarm codes and code changes are maintained by Systems and Operations. The James Madison University Police Department monitors the intrusion alarms and performs onsite investigations when alarms are triggered, and reports findings to central IT.

Any person entering an IT Facility for whom access has not been granted is a visitor and is escorted by a person granted access. An entry log is maintained in each facility and each visitor is logged with the following information:

a. Date
b. Time In
c. Time Out
d. Name
e. Company (if a vendor or contractor)
f. Reason for Visit
g. Contact/Escort

Entry logs are reviewed periodically and retained for auditing purposes.

Photography by visitors is prohibited. Persons granted access may take photos only for operational purposes. Such photos are sensitive data and must receive the same protection as any other infrastructure documentation that may have security implications.

Surveillance cameras are installed in IT Facilities to help ensure positive identification of individuals entering and exiting.

3. Environmental Monitoring

IT Facilities include environmental monitoring to detect conditions that could result in damage to equipment or loss of data. This monitoring includes ambient temperature, humidity, and the presence of water at the lowest point of the room, as may occur with a leaking pipe, roof, etc. The monitoring system generates alerts for abnormal conditions to be received by the Responsible Party. For alerts outside normal business hours, the Responsible Party designates on call personnel who respond within one hour of receiving the alert.

4. Fire Suppression

IT Facilities contain fire suppression systems appropriate for the application. These include dry pipe sprinkler systems or chemical agent systems. Due to the possibility of accidental activation or leaks, wet pipe sprinklers typically installed in commercial buildings are not suitable for IT Facilities. If retrofitting the fire suppression in an existing IT Facility is impossible, the sprinkler heads may be upgraded to 200°F or higher activation temperature (green or blue glass bulbs) and protected with high strength metal sprinkler guards capable of preventing activation by ladders, projectiles, and other hazards. Concealed sprinkler heads may be used as well, provided they activate at 200°F or higher, have covers flush with the ceiling, and the part above the ceiling is protected from work that may be performed there.

5. Emergency Power

IT Facilities are located in buildings served by standby generators and are fed by electrical circuits protected by the generators. An uninterruptible power supply (UPS) of sufficient capacity to serve the load of the equipment is installed, and it provides sufficient battery backup run time, at minimum, for the standby generators to come online during an outage of utility power, and for the correction of human error such as inadvertently switching off both utility and standby power sources. The environmental monitoring in data centers detects and notifies when the power source (utility or generator) changes.

6. Computer Room Air Conditioning

IT Facilities contain purpose-built air conditioning systems to adequately control temperature and humidity. They are sized to cool the ambient space, remove the heat generated by the electronic equipment, plus provide adequate reserve margin for unanticipated growth or operating conditions. There is redundancy built into these systems or alternative methods of cooling made available as needed so that maintenance can be performed or failures can be tolerated without loss of temperature control.

7. Documented Procedures

Responsible parties must have written procedures for managing the physical and environmental security of IT Facilities to help prevent loss of data, unavailability of systems or data, and negatively impacting the integrity of data. Procedures must be in accordance with this Standard and provided to IT upon request.