WAYNE STATE
UNIVERSITY
Computing & Information Technology

Standard for Physical & Environmental Protection

Purpose

This standard establishes the need for University computing facilities that store or process University information to be physically secure from disclosure, alteration, or loss of data, and establishes the authority for maintaining compliance with the security controls selected to achieve this security.

Scope

The scope of this standard covers all physical server environments located at Wayne State University where university data is stored or processed, whether occurring in central or distributed University IT departments. Desktop computing is not in scope of this standard.

Roles and Responsibilities

All University IT staff, including University IT management, will maintain their server computing environments in a secure physical location that is resistant to theft, burglary, fire, water damage, electrical issues, and other relevant physical and environmental risks.

Because physical security procedures and controls are needed for compliance with federal requirements, University management will ensure University data processing facilities are physically secured to the minimum standards set forth in the associated standards. Additionally, management will account for physical security requirements when establishing or significantly altering electronic information systems that are in scope of this standard.

The C&IT Information Security Office will, on review of any facilities that are non-compliant, terminate network access to any server or system which inherits unacceptable risk of loss as a result of being housed in a non-compliant location or facility.

Resource permitting, C&IT Critical Facilities staff will provide input and guidance to distributed units on the implementations of technical controls which have been successfully used in the C&IT datacenter environment.

Physical & Environmental Standards, Procedures, and Guidelines

Detailed procedures, standards, and guidelines will be authored and maintained by the C&IT Information Security Office outlining the specific physical security controls to be implemented, along with appropriate guidance. New or modified procedures, standards and guidelines will be communicated to all University IT staff once approved by the C&IT Risk & Security Oversight Committee.

Organizational Coordination
The C&IT Information Security Office will solicit feedback from on-campus IT units regarding the effectiveness and applicability of this standard and related standards, taking it into consideration during periodic standard review. This standard and associated documents will be openly published and communicated to all IT staff at a minimum of an annual basis.

Compliance
All university units are required to be in compliance with this standard and any associated standards. Any exceptions to this standard must be approved by the C&IT Information Security office, will be given a deadline for proper compliance, and will be reviewed on an annual basis.

Standard Review
This standard and any associated procedures, standards, and guidelines will be reviewed at a minimum on an annual basis by the C&IT Risk & Security Oversight Committee.

Standards for Facility Access Control
Facilities must use and maintain the following controls to protect against personnel threats:

1. Limiting Access. Facilities must be in an indoor, enclosed space or room with defined entry points. Access to the facility must be controlled by doors utilizing mechanical or electronic locking mechanisms which remain closed and locked during regular facility operation.

2. Authorizing Access. Access to any facilities must be restricted to approved and authorized individuals. Individuals requesting authorization must have a valid business need for facility access, and facility owners must verify the validity of any access requests. Facility owners must create and maintain a list of individuals that are permitted to enter the facility which must be reviewed at minimum of a quarterly basis, removing access from individuals no longer requiring it.

3. Providing Access. Facility owners or their designee(s) must issue and revoke credentials for facility access such as keys, unique codes, or RFID cards. These credentials must be secured by the facility owner when not assigned and reconciled against credential inventory on a minimum of a quarterly basis. Credentials must be changed when lost, compromised, or when an assigned individual is transferred or removed from the organization.

4. Monitoring Access. Access into facilities must be monitored for abnormal behavior or suspicious activity. Facility owners must maintain a log for a minimum of 90 days for all access into a facility, and this log must be reviewed at a minimum of a quarterly basis. Identified abnormal behavior must be reported to the C&IT Information Security Office for official incident response action.

5. Controlling Visitor Access. Facility owners must maintain a visitor log for any individuals entering a facility that have not been given prior authorized access, such as vendors or guests, or for access to any designated area of the facility that is public. The visitor log must contain the name and organization of the visitor, as well as the times signed in and out, the reason for the visit, and the name and signature of the authorized individual sponsoring the guest visit. Visitors must be accounted for at all times while in the facility by being accompanied in person and/or monitored via a recorded surveillance camera. Visitor logs must be maintained for a minimum of 90 days and reviewed at a minimum of a quarterly basis.

Standards for Facility Environmental Controls
Facilities must use and maintain the following controls to protect against environmental threats:

1. Emergency Lighting. In the event of a power failure, emergency lighting must exist and automatically activate to allow facility occupants to see and navigate emergency egress routes to designated exits.

2. Temperature and Humidity Control. Dedicated HVAC equipment or control panels must exist and be able to provide a reliable source of climate-controlled air to the facility to achieve:
   a. Ambient temperature between 65 and 75 degrees Fahrenheit.
   b. Ambient relative humidity between 40 to 60 percent.

   Temperature and humidity levels must be monitored on a minimum of an hourly basis, with the facility owner or their designee being notified if these conditions violate the above thresholds.

3. Fire Protection. Facilities must utilize fire detection methods that notify WSU Public Safety in the event of detected combustion or fire. Fire suppression methods must also be used, and can consist of gaseous fire suppressant, sprinklers, or handheld extinguishers located and conspicuously marked both inside and immediately outside the facility.

4. Water Damage Protection. Master shutoff valves for building water mains and supply lines must be identified and documented by the facility owner, and proper drainage must exist in the facility to remove water in the event of flood or leak.

Additional Standards for Enhanced Facilities
University facilities that store or process confidential data must occur within an enhanced facility, which is subject to the following additional security controls:

1. Network Access Control. Physical access to network cabling and electronics is restricted. Server cabinets must remain locked and overhead cable trays used for communication wires.

2. Output Device Control. Output devices displaying confidential information, such as monitors and printers, must be kept in an area of the facility with separate and more granular access controls to restrict the personnel that can view them.

3. Surveillance. Surveillance cameras must be placed and focused on each ingress and egress location in the facility, as well as any areas in the facility where confidential information is stored or processed. Cameras should be able to distinguish individual features and allow for identifying individuals in the event of unauthorized access or suspected incident. Camera footage must be retained for at least 30 days and be stored on a central system.

4. Alarm Monitoring. Intrusion alarms and surveillance cameras must be monitored on a continual basis by facility staff or WSU Public Safety.

5. Power Protection. Multiple power sources must be utilized when distributing power to the facility, coming from different sources and utilizing different physical paths. The facility must have an uninterruptable power supply (UPS) capable of handling the normal load of the facility until an

orderly system shutdown can be completed, or long-term power is available via a self-contained, sustainable generator system.

6. Emergency Shutoff. An Emergency Power Off ("EPO") device must be placed at each ingress and egress point of the facility and be conspicuously marked. Each EPO device must immediately turn off all power to the facility on activation, as well as utilize a cover or mechanism to prevent accidental activation.

7. Automatic Fire Suppression. Fire detection and suppression systems must activate without human intervention in the event of detected fire or combustion. Automatic discharge of fire suppressant must happen after audible and visual alarms are activated and a delay timer of 30 seconds is allowed to expire.

8. Alternate Work Sites. Individual managers use discretion to select alternate work sites for their employees in the event their normal work site is uninhabitable. Managers are responsible for assessing the feasibility of any selected alternate work sites with regards to security and connectivity.

Non-Compliance
The C&IT Information Security Office may limit access to or from a system if it does not meet the above guidelines.

Exceptions
Exceptions to these standards may be granted by the Information Security Office given business justification and a satisfactory risk assessment. In such cases, the system owner shall acknowledge the risk and take responsibility for any breaches, incidents, or compromises that occur as a result of not utilizing a supported operating system.