1.0 PURPOSE

The purpose of this policy is to provide physical and environmental protection (PE) requirements for Ohio Department of Administrative Services (DAS)-managed information systems and for the facilities in which they operate. Documented PE security controls are needed to ensure information systems are properly protected against physical and environmental threats.

A glossary of terms found in this policy is located in Section 8.0 Definitions. The first occurrence of a defined term is in **bold italics**. In addition, references to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” family identifiers and control numbers are provided in parentheticals next to requirement headers, where applicable.

2.0 SCOPE

The scope of this policy includes any DAS-managed information system and the facility in which it operates. This policy also applies to DAS data owners, system and service owners, and extends to external service providers.

For the purposes of this policy, ‘facility’ refers primarily to physical locations containing concentrations of DAS-managed information system resources including, for example, data centers, server rooms, rooms containing sensitive network, telecommunications, or electrical equipment, and mainframe computer rooms. ‘Managed service partner facility’ refers to these same physical locations when operated by an external entity through agreement with DAS.

This policy is intended to detail required physical and environmental security controls, but is not intended to supersede local or state building regulations, or fire or electrical codes.
3.0 BACKGROUND

Physical and environmental security controls are implemented to protect facilities as well as DAS-managed information systems. These controls are necessary to help prevent interruptions in information technology (IT) services, physical damage, unauthorized disclosure of information, loss of control over information system integrity, and theft.

4.0 REFERENCES

4.1 Ohio IT Standard; ITS-SEC-02; Security Controls Framework: This state IT standard specifies the minimum requirements for information security in all agencies and identifies the NIST SP 800-53 as the framework for information security controls implementation for the state.

4.2 National Institute of Standards and Technology Special Publication 800-53; Security and Privacy Controls for Federal Information Systems and Organizations: NIST SP 800-53 provides guidelines for selecting and specifying security controls for federal government information systems.

4.3 Ohio Administrative Policy IT-05, Disposal, Servicing and Transfer of IT Equipment: Ohio IT Policy IT-05 mitigates risk with regard to state data, licensed software and intellectual property, and rechargeable batteries and other hazardous materials in the disposal, servicing or transfer of state agency IT equipment.

4.4 Ohio Administrative Policy IT-13, Data Classification: Ohio Administrative Policy IT-13 provides a data classification methodology to state agencies for the purpose of understanding and managing data and information systems with regard to their level of confidentiality and criticality.

4.5 DAS Policy 2100-08; Risk Assessment: Provides risk assessment requirements for DAS-managed system assets. The requirements address preparing for, conducting, communicating and maintaining a risk assessment.

4.6 National Fire Protection Association (NFPA) 70; National Electric Code (NEC): This is the nationally adopted benchmark for safe electrical design, installation and inspection.

5.0 POLICY

Each DAS-managed information system and the facility in which it operates shall adhere to the following physical and environmental protection requirements.
5.1 **Physical Access Authorizations (PE-2):** This control applies to all facilities where DAS-managed information systems operate, including the facilities of external service providers. For each facility, the facility manager shall:

5.1.1 Develop, and maintain a list of approved individuals with authorized access to the facility.

5.1.2 Issue authorization credentials for facility access. Authorization credentials include, for example, badges, identification cards, and smart cards. For each facility, the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) shall be commensurate with the results of the data classification as outlined in Ohio Administrative Policy IT-13, “Data Classification,” as well as the **system classification**.

5.1.3 Review the access list detailing authorized facility access by individuals at least quarterly or more frequently if required by other regulations.

5.1.4 Remove individuals from the facility access list when access is no longer required.

5.1.5 Enforce physical access authorizations to information systems in addition to physical access controls for sections of the facility where federal tax information (FTI) is received, processed, stored, or transmitted or where dictated based on the results of the risk assessment, conducted in accordance with DAS Policy 2100-08, “Risk Assessment,” and data classification.

5.1.6 For information systems subject to the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy, physical access to locations housing such systems shall be based on role.

5.1.7 Unescorted access to FBI CJIS information systems shall be restricted to only those individuals with formal authorizations for the information system. All other individuals requiring access to the information system must be escorted.

5.2 **Physical Access Control (PE-3):** This control applies to all facilities where DAS-managed information systems operate, including the facilities of managed system providers. For each facility, the facility manager shall:
5.2.1 Enforce physical access authorizations at entry/exit points by:

5.2.1.1 Verifying individual authorizations before granting access to the facility; and

5.2.1.2 Controlling ingress/egress to the facility using systems/devices or guards.

5.2.2 Maintain physical access audit logs for entry/exit points.

5.2.3 Provide security safeguards to control access to areas within the facility officially designated as publicly accessible.

5.2.4 Escort visitors and monitor visitor activity.

5.2.5 Secure keys, combinations, card readers and other physical access devices.

5.2.6 Inventory physical access devices at least annually.

5.2.7 Change combinations at least annually and also when combinations are compromised; or when an individual who knows the combination retires, terminates employment, or transfers.

5.2.8 When a key is lost or stolen, re-key or replace the associated lock.

5.2.9 The facility manager shall ensure regularly scheduled and random physical security checks occur at the physical boundary of facilities housing FBI CJIS information systems.

5.2.10 Facilities housing FBI CJIS information systems shall employ guards and/or alarms to monitor every physical access point to the facility 24 hours per day, 7 days per week.

5.3 **Access Control for Transmission Medium (PE-4):** Commensurate with the results of the risk assessment and data classifications for information systems housed at DAS or external service provider facilities, physical access controls shall be implemented for information system distribution or transmission lines. Security safeguards to control physical access to information system distribution and transmission lines include, for example: locked wiring closets; disconnected or locked spare network jacks; and/or protection of cabling by conduit or cable trays.
5.4 **Access Control for Output Devices (PE-5):** Physical access to information system output or output devices shall be controlled to prevent unauthorized individuals from obtaining the output. Monitors, printers, copiers, scanners, fax machines, and audio devices are examples of information system output devices.

5.5 **Monitoring Physical Access (PE-6):** Each DAS or external service provider facility shall:

5.5.1 Monitor physical access to the facility where the information system resides to detect and respond to physical security incidents;

5.5.2 Monitor and respond to physical intrusion alarms and surveillance equipment;

5.5.3 Review physical access logs for security violations or suspicious activity at least quarterly; and

5.5.4 Coordinate results of reviews and investigations with the Office of Information Security and Privacy (OISP) Enterprise Information Security and Privacy Incident Response Team (SIRT).

5.6 **Visitor Access Records (PE-8):** Visitor access records shall include name and organization of person visiting, visitor signature, form of identification, date of access, entry and departure times, purpose of visit, and the name and organization of the person visited. Visitor access records are not required for publicly accessible areas. Each DAS or external service provider facility shall:

5.6.1 Maintain visitor access records for five years; and

5.6.2 Review visitor access records at least quarterly.

5.7 **Power Equipment and Cabling (PE-9):** In compliance with applicable building codes and in alignment with data center industry best practices for the advertised tier level, power equipment and power cabling at DAS or external service provider facilities shall be protected from damage and destruction.

5.8 **Emergency Shutoff (PE-10):** Each DAS or external service provider facility shall implement the following emergency shutoff controls, except where not required by
the regulations outlined in NFPA 70; NEC Article 645, Information Technology Equipment:

5.8.1 Provide the capability to shut off power to information systems or information system components in emergency situations;

5.8.2 Appropriately place emergency shutoff switches or devices to facilitate safe and easy access for personnel; and

5.8.3 Protect emergency power shutoff capability from unauthorized activation.

5.9 **Emergency Power (PE-11):** DAS or external service provider facilities shall provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system or an uninterrupted transition to long-term alternate power in the event of a primary power loss.

5.10 **Emergency Lighting (PE-12):** In accordance with applicable building codes, DAS or external service provider facilities shall employ and maintain automatic emergency lighting that activates in the event of a power outage or disruption that covers emergency exits and evacuation routes within the facility.

5.11 **Fire Protection (PE-13):** DAS or external service provider facilities shall:

5.11.1 Employ and maintain fire suppression and detection devices/systems that are supported by an independent energy source; and

5.11.2 Employ and maintain an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

5.12 **Temperature and Humidity Controls (PE-14):** DAS or external service provider facilities shall:

5.12.1 Maintain temperature and humidity levels within the facility in accordance with the optimal operating range of the information system components.

5.12.2 Monitor facility temperature and humidity levels.

5.13 **Water Damage Protection (PE-15):** DAS or external service provider facilities shall protect information systems and information system components from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to appropriate personnel.
5.14 **Delivery and Removal (PE-16):** DAS or external service provider facilities must authorize, monitor, and control information system components entering and exiting the facility delivery areas and maintain records of them.

5.14.1 Each DAS or external service provider facility shall define and document an auditable procedure that details the requirements for information system components entering and exiting the facility as well as the handling of data that may be stored on the components in accordance with Ohio Administrative Policy IT-05, “Disposal, Servicing and Transfer of IT Equipment.”

5.15 **Alternate Work Site (PE-17):** While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Alternate work sites may include, for example, government facilities or private residences of employees. DAS or external service provider alternate work sites shall:

5.15.1 Identify and employ security controls at the alternate work site in accordance with the information system risk assessment and data classification.

5.15.2 Assess, as feasible, the effectiveness of security controls at alternate work sites.

5.15.3 Provide a means for workers at alternate work sites to communicate with information security personnel in case of security incidents or problems.

5.16 **Location of Information System Components (PE-18):** DAS or external service provider facilities must position information system components within the facility to minimize potential damage from physical and environmental hazards (e.g., locating components in core areas of the facility, choosing places within the facility that emergency crews can access, avoiding proximity to water sources and exposure to environmental conditions), and to minimize the opportunity for unauthorized access.

5.16.1 Risk mitigation strategies for facilities housing FBI CJIS information systems must account for physical and environmental hazards to the facility itself.
6.0 PROCEDURES

As of the effective date of this policy, any new external service provider contractual agreements, that involve the use of facilities to house or operate DAS-managed information systems, shall include a requirement to comply with this policy.

7.0 COMPLIANCE

As of the effective date of this policy, some DAS or external service provider facilities may not be completely aligned to the physical and environmental protection requirements outlined in the policy. A general implementation framework for the requirements of this policy includes:

7.1 For DAS-managed information system or external service provider facilities that are already operational, the requirements outlined within this policy shall be implemented within six months from the effective date of the policy or within a mutually agreed to timeframe with the external service provider not to exceed one year from the effective date of the policy.

7.2 All planned and future DAS-managed information system or external service provider facilities shall immediately comply with the requirements outlined in this policy.

8.0 DEFINITIONS

Availability - Ensuring timely and reliable access to and use of information.1

Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.2

DAS-managed Information Systems - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.3 For the purposes of this policy, primary responsibility for managing these systems may be assigned to DAS OIT personnel or other outside entities.

Data - Coded representation of quantities, objects and actions. The word, “data,” is often used interchangeably with the word, “information,” in common usage and in this policy.

Disposal - The final transfer of ownership or custody of an information technology device.

2 Ibid.
3 Ibid.
Environmental - Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system.\(^4\) Environmental controls include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility.\(^5\)

External Service Provider – An entity outside State of Ohio government that provides external information system or service capabilities to DAS by contract.

Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy - The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of Criminal Justice Information (CJI), whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. The policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.\(^6\)

Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.\(^7\)

Physical – Security controls that address elements such as physical access authorizations, transmission mediums, output devices, monitoring, visitor control, visitor access, and alternate work sites. Physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures).\(^8\)

---


\(^{7}\) Ibid.

**Risk Assessment** - The process of identifying, prioritizing, and estimating risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system.  

**Services** - The application of business and technical expertise to enable organizations in the creation, management and optimization of or access to information and business processes.

**System Classification** - Refers to the process of assessing the potential impact to confidentiality, integrity and *availability* of the evaluated system. NIST SP 800-53 refers to Federal Information Processing Standards (FIPS)-199, which is the federal guideline for assessing and classifying information systems. DAS OISP plans to develop further guidance around system classification, but agencies can utilize the FIPS-199 publication until further guidance is released.

**Service Owner** - A service owner is responsible for the delivery (design, performance, integration), continual improvement and management of assigned IT services.

### 9.0 INQUIRIES

Direct inquiries about this policy to:

Office of Information Security & Privacy  
Office of Information Technology  
Ohio Department of Administrative Services  
30 East Broad Street, 19th Floor  
Columbus, Ohio 43215  

614.644.9391 | state.isp@das.ohio.gov

DAS Policies may be found online at [http://das.ohio.gov/Divisions/Administrative-Support/Employees-Services/DAS-Policies](http://das.ohio.gov/Divisions/Administrative-Support/Employees-Services/DAS-Policies)

Additional information regarding the Office of Information Security & Privacy may be found online at [infosec.ohio.gov](http://infosec.ohio.gov).

---

10.0 REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/22/2017</td>
<td>Original Policy.</td>
</tr>
<tr>
<td>12/22/2018</td>
<td>Scheduled policy review.</td>
</tr>
</tbody>
</table>

11.0 ATTACHMENTS

None.