## GOVERNANCE

This document is governed by the IT Governance policy which provides the following guidance:

a. Roles and Responsibilities
b. Policy Control Application
c. Policy Compliance Requirements
d. Policy Exemptions or Exceptions
e. Policy Reviews and Updates

## SCOPE

This policy covers all State information and information systems to include those used, managed, or operated by a contractor, an agency, or other organization on behalf of the State. This policy applies to all State employees, contractors, and all other users of State information and information systems that support the operation and assets of the State.

## PE-1 POLICY AND PROCEDURES

All information assets that process, store, receive, transmit or otherwise impact the confidentiality, integrity, and accessibility of State data shall meet the required security controls defined in this policy document based on the National Institute of Standards and Technology (NIST) SP 800-53 r5, Security and Privacy Controls.

This document addresses the procedures and standards set forth by the State to implement the family of Physical and Environmental Protection controls at the organization, process and/or system level for all State data and information assets.

The State has adopted the Physical and Environmental Protection security principles established in NIST SP 800-53, r5 “Physical and Environmental Protection” control guidelines as the official policy for this security domain. The “PE” designator identified in each control represents the NIST-specified identifier for the Physical and Environmental Protection control family. A designator followed by a number in parenthesis indicates a control enhancement that provides statements of security and privacy capability that augment a base control. Only those control enhancements associated with the moderate level controls are listed. Should an executive-branch agency be required to address other control enhancements for a control item, the organization will be responsible for writing an additional policy to meet that requirement.

The following subsections in this document outline the Physical and Environmental Protection requirements the State and executive-branch agencies shall implement and maintain to protect the privacy and security of sensitive and confidential information and prevent unauthorized data access.

This policy and associated procedures shall be reviewed at least every three (3) years or following agency-defined events requiring off-cycle review and changes.

This policy and associated procedures shall be developed, documented, and disseminated by the Secretary of the Alabama Office of Information Technology, or other designated organizational officials at the senior leadership level.

## PE-2 PHYSICAL ACCESS CONTROL

Access to digital and non-digital media shall be restricted to authorized individuals only, using State-defined security measures:

a. Access policies shall be developed for authorized individuals and visitors to State facilities;
b. Risk assessment shall guide the selection of media, and associated information contained on that media requiring restricted access;
c. System Owners shall document policies and procedures for media requiring restricted access, individuals accessing media, and specific measures to restrict access;
d. Authorization credentials (e.g., badges, identification cards, and smart cards) shall be issued to everyone accessing a restricted area;
e. Everyone within a State building must display either a State Identification (ID) Badge or a numbered and current visitor badge. These badges are the property of the State and are provided to employees and visitors as a convenience. Badges must always be visible above the waist when inside State buildings and not visible to the public outside of State buildings;
f. The access level provided to individual users shall not exceed the level required to complete their job responsibilities;
g. The access level shall be reviewed and approved before access is granted;
h. Keys, badges, access cards, and combinations shall be issued only to personnel with duties requiring that specific access;
i. Keys, combinations, and other physical access devices shall be secured to prevent unauthorized access to agency facilities and assets. These shall also be inventoried on an agency-defined frequency. Unauthorized duplication of keys is prohibited. All requests for duplicate keys shall be submitted to the State locksmith for review, approval, and fulfillment;
j. Keys shall be retrieved from the employee when they retire, terminate employment, or transfer to another position;
k. Keys and combinations shall be changed at least annually for secure areas housing systems with sensitive or confidential data;
l. Authorizations and requirements for access shall be coordinated with facility and personnel security managers;
m. Access lists and authorization credentials shall be reviewed and approved quarterly to ensure the following:
    i. Access shall be limited to only authorized personnel;
    ii. The level of access provided to individual users shall be consistent with the individual's job responsibilities; and
    iii. Access rights shall be promptly removed for terminated and transferred personnel or for personnel no longer requiring access to the facility where the information system resides.
n. Enforce physical access authorizations to the information system in addition to the physical access controls for the facility at spaces where sensitive or confidential data is received, processed, stored, or transmitted.

## PE-3 – PHYSICAL ACCESS CONTROL

Sites and facilities staffed and containing information technology equipment shall be carefully evaluated to identify and implement controls to protect staff and State resources from environmental threats, physical intrusion, and other threats.

a. Organizations shall safeguard sites, buildings and locations housing its information technology assets;

b. All locations that house sensitive or confidential data shall be designed and secured in accordance with the highest level of information being protected;
c. Physical access authorizations at entry/exit points to facilities where the information systems that receive, process, store, or transmit sensitive or confidential data shall verify individual access authorizations before granting facility access, and control ingress/egress to the facility using physical access control systems/devices or guards;
d. Authorized individuals may include State and agency employees, contractors, vendors, and customers;
e. Physical access controls should include visible identification such as a driver's license or other picture identification, e.g., agency badge. An audit trail of physical access for all individuals to data centers shall be maintained including entry and exit dates and times;
f. The number of people with physical access to areas housing computer equipment shall be controlled to reduce the threats of theft, vandalism, and unauthorized system access. The following measures should be considered to control and restrict access to computing facilities:
    i. Access shall be restricted to individuals with authorized purposes;
    ii. Instructions shall be issued to visitors explaining security requirements and emergency procedures;
    iii. Visitors shall be escorted and wear visible identification clearly indicating their restricted status;
    iv. Organizations shall store resources in lockable storage where the physical security controls are sufficient to protect the resources from theft; and
    v. Lockable file cabinets shall be used to store sensitive or confidential data such as paper documents and computer media in a manner commensurate with the information's classification status.
g. Video cameras and/or access control mechanisms shall be used to monitor individual physical access to sensitive areas;
h. The use of personal cameras, video recorders, and mobile computing devices shall be restricted in high security locations to protect the information stored;
i. Duress alarms shall be used in areas where the personnel safety is a concern, and alarms shall be provisioned to alert staff, law enforcement, the fire department, and other first responders;
j. Videoconference calls containing sensitive or confidential information shall be made in a secure area; and
k. Facilities housing sensitive or confidential data shall include, but not be limited to, and/or require the following security measures at each location:
    i. Clearly defined, layered security perimeters to establish multiple barriers
    ii. Physical walls
    iii. Card-controlled gates and doors
    iv. Bars, alarms, locks, etc.
    v. Bollards (a sturdy, short, vertical post used to block vehicle entrances)
    vi. Video cameras and intrusion security system
    vii. Staffed reception desk
    viii. Fire doors on a security perimeter shall be equipped with alarms and automatically closing door(s)

## PE-4 – ACCESS CONTROL FOR TRANSMISSION

Physical access to information system distribution and transmission lines within agency facilities shall be controlled:

a. Protective measures to control physical access to information system distribution and transmission lines shall include the following:
    i. Locked wiring closets;
    ii. Disconnected or locked spare network jacks; and
    iii. Protection of cabling by conduit or cable trays.
b. Publicly accessible network jacks in data centers shall provide only internet access by default unless additional functionality is explicitly authorized; and
c. Physical access to networking equipment and cabling shall be restricted to authorized personnel.

## PE-5 - ACCESS CONTROL FOR OUTPUT DEVICES

Physical access to information system output devices, such as computer monitors, copiers, and printers, shall be controlled to prevent unauthorized users from obtaining the output.

a. Where technically configurable, enable security functionality on printers, copiers, and peripherals to require users to authenticate with the device via a PIN or hardware token to access the device;
b. Control physical access to output devices by placing devices in controlled areas with keypad access controls or limiting access to individuals with certain types of badges; and
c. Control physical access to monitors through privacy screens or by re-positioning monitors away from the view of unauthorized users.

## PE-6 – MONITORING PHYSICAL ACCESS

Physical access to information systems shall be monitored to detect and respond to physical security incidents.

a. Coordination with facility management and personnel security management personnel shall occur when responsibilities are in different organizations;
b. Physical access logs shall be reviewed at least monthly by the agency Security Liaison or other designated agency official at management level;
c. Investigations of apparent security violations or suspicious physical access activities shall be conducted. Investigations and results of reviews shall be coordinated with the organization's incident response capability:
    i. Remedial actions identified because of investigations shall be developed and implemented; and
    ii. Incident investigations shall follow the Incident Response Policy requirements.
d. Investigation and response to detected physical security incidents, including apparent security violations or suspicious physical access activities shall be part of the agency's incident response procedures; and
e. Operational procedures shall be developed to document how these individuals shall respond to

physical access incidents.

**PE-6 (1) – MONITORING PHYSICAL ACCESS | INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT**

Physical intrusion alarms and surveillance equipment shall be installed and monitored. Automated mechanisms to recognize potential intrusions and initiate designated response actions shall be employed.

**PE-8 – VISITOR ACCESS RECORDS**

Security access logs for areas containing sensitive and/or confidential information and information technology equipment shall be actively monitored using visitor logs, including computing facilities containing State-owned equipment and information. Visitor logs must address the following requirements:

a. Name and organization of the person visiting;
b. Visitor signature;
c. Type of ID provided and who verified;
d. Access date, entry, and departure times;
e. Visit purpose;
f. Name of person visited;
g. The visitor access records shall be reviewed at least monthly;
h. Anomalies in visitor access should be reported to the organization's facility management and agency personnel (for vendor computing facilities containing State managed data); and
i. Visitor access records for facilities housing any federal data shall be maintained for at least five (5) years. All other facilities access records shall comply with the agency's records retention policies.

**PE-9 – POWER EQUIPMENT AND CABLING**

Power equipment and cabling for information systems shall be protected from damage and destruction:

a. Multiple electric feeds, which are physically separated, shall be employed to avoid a single point of failure in the power supply and to help ensure that power continues to flow in the event one of the cables is cut or otherwise damaged;
b. Both power and communication lines should be protected; and
c. Automatic voltage controls for critical system components shall be used to ensure continuous power if voltage fluctuates to unacceptable levels.

**PE-10 – EMERGENCY SHUTOFF**

Power shut off to the information system or individual system components in emergency situations shall be accomplished using emergency power switches located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. These switches shall be in a visible location and clearly labeled, with the emergency power-off capability protected from accidental or unauthorized activation.

Locations for emergency power shutoffs must be documented and personnel informed of the emergency power shutoff locations and procedures to operate them safely.

**PE-11 – EMERGENCY POWER**

Critical information technology systems shall be protected from damage and data loss by installing and routinely testing a source of continuous power to ensure the systems perform during power outages and electrical anomalies.

a. The three primary methods for providing continuous power are:
    i. Multiple electric feeds to avoid a single point of failure in the power supply;
    ii. Uninterruptible power supply (UPS); and
    iii. Backup generator(s).
b. Each organization shall examine the availability requirements for critical equipment and determine the most suitable combination of methods relevant to its mission;
c. Emergency power requirements for critical systems shall be analyzed based on the following best practices:
    i. Use of a UPS is usually required to avoid abnormal shutdowns or to provide a clean power source during brownouts or surges;
    ii. Contingency plans that include procedures to follow if the UPS fails; and
    iii. Periodic inspections of UPS equipment to ensure the equipment can sustain the power load of the systems it supports and that it is serviced according to the manufacturer's specifications.
d. Backup generators shall be used in combination with a UPS when requirements demand high availability and continuous processing in the event of a prolonged power failure;
e. Organizations requiring a backup generator should ensure:
    i. Contingency plans shall include procedures if the backup generator fails;
    ii. The generator capacity is appropriate to sustain the power load required by supported equipment for a prolonged period;
    iii. The generator is tested at least quarterly according to the manufacturer's specifications; and
    iv. Generators are serviced within manufacturer's specifications and have an adequate fuel supply for prolonged performance.

**PE-12- EMERGENCY LIGHTING**

Automatic emergency lighting that activates during a power outage or disruption and covers emergency exits and evacuation routes within the facility shall be used and maintained.

The automatic emergency lighting systems shall be tested at least annually to ensure they are fully operational and the test results should be documented.

**PE-13 – FIRE PROTECTION**

This control applies primarily to facilities containing concentrations of information system resources including, but not limited to, data centers, server rooms, and network closets.

Security controls shall be implemented to assure continual service of critical production systems,

including controls monitoring, and alerting to log intrusions, fires, explosives, smoke, water, dust, vibrations, chemicals, electrical effects, electrical supply interferences, and electromagnetic radiation.

a. Fire detection and suppression devices supported by an independent power source, such as a dry pipe sprinkler system shall be installed and maintained;
b. Fire-resistant storage for documents and media containing information critical to business function shall be provided where required;
c. Fire extinguishers must be checked annually with the inspection date documented on the extinguisher; and
d. All fire protection resources must be tested annually in accordance with local or state fire regulations to ensure they can be successfully activated when needed.

**PE-13 (1) – FIRE PROTECTION | DETECTION SYSTEMS – AUTOMATIC ACTIVATION AND NOTIFICATION**

Fire detection devices/systems should activate automatically and notify emergency personnel and defined emergency responder(s) when the facility is not staffed on a continuous basis and an event is detected.

**PE-14 – ENVIRONMENTAL CONTROLS**

Automatic temperature and humidity controls shall be implemented and maintained in data centers to prevent fluctuations potentially harmful to equipment.

Temperature and humidity monitoring shall be employed that provide an alarm or other notification when temperature and humidity settings are exceeded due to heating, ventilation, or air conditioning (HVAC) failures and may impact information assets.

**PE-15 – WATER DAMAGE PROTECTION**

Measures shall be taken to prevent water damage in the design requirements for secure data storage, and the facility must have master shutoff valves accessible, functioning, and known to key personnel, to protect the information system from water leakage.

**PE-16 – DELIVERY AND REMOVAL**

Access to delivery areas shall be restricted and isolated from the information system and media libraries to effectively enforce authorizations for entry and exit of information system components.

All information system components and packages delivered to or removed from the facility shall be authorized and controlled with records of those items entering and exiting the facility maintained.

**PE-17 – ALTERNATE WORK SITE**

The State shall provide readily available alternate work locations (e.g., governmental offices, commercial locations, employee homes, etc.) as part of contingency operations:

a. Alternate work sites should be determined, approved, and documented.
b. The effectiveness of controls at alternate work sites shall be assessed, as feasible. Alternate work sites shall be equipped with any equipment needed to resume temporary operations such

as telecommunications services including but not limited to alternative telephone services, wireless networking, satellite, and radio that will allow employees to communicate with information security and privacy personnel in case of security incidents or problems.

c. Organizations shall secure and protect communications with information resources while personnel are working at off-site locations. Remote access security requirements are defined in the State's Access Control Policy.
d. Alternate work sites must meet State and federal security control requirements. If the organization does not have direct control over the remote location, the organization shall contract with the owner and stipulate the access controls and protection the owner shall implement.
e. Alternate work sites must have at least sufficient physical access controls to the site and the data contained, with design requirements for secure data storage.
f. Equipment being used or stored at an individual alternate work site, such as hotel, home, or other alternate site, must be secured when not in use.
g. Equipment transported in vehicles must be hidden from casual view and must not be stored in vehicles overnight.

## PE-18 – LOCATION OF SYSTEM COMPONENTS

Information system components must be positioned within the facility to minimize potential damage from physical and environmental hazards and to minimize unauthorized access opportunities.

## POLICY OWNER

Secretary of Office of Information Technology (OIT)

## MATERIAL SUPERSEDED

This current policy supersedes all previous versions. All State agencies and contractors/vendors of the State are expected to comply with the current implemented version.

## REVISION HISTORY

| Revision Date | Summary of Change |
|---|---|
| 12/31/2024 | Policy Update |

## REMAINDER OF PAGE LEFT INTENTIONALLY BLANK

**APPROVED BY**

| | |
|---|---|
| Signature | Daniel Urquhart |
| Approved by | Daniel Urquhart |
| Title | Secretary of Office of Information Technology (OIT) |
| Date Approved | 01/15/2025 |

**REMAINDER OF PAGE LEFT INTENTIONALLY BLANK**