State of Maryland

STANDARD

PHYSICAL & ENVIRONMENTAL PROTECTION

Document No.	Last Updated	Prepared By
MD-STD-311-PE-01	02/18/2026	DOIT OSM

Physical and environmental protection, as integral components of Zero Trust Architecture (ZTA), are fundamental to safeguarding assets, ensuring operational continuity, and preventing security breaches by enforcing strict access controls, continuous monitoring, and real-time threat detection to mitigate risks both physically and digitally.

PURPOSE AND SCOPE

Purpose	This standard provides the technical and operational specifications needed to mitigate risks associated with unauthorized access, environmental hazards, natural disasters, and infrastructure vulnerabilities.
Scope	This standard addresses safeguarding facilities, systems, and infrastructure from physical threats.
Applicability	This standard applies to all units of State government (as defined in SF&P 3.5-101(g)), hereafter referred to simply as “agencies.”
Related Policy	This standard is part of a broader policy suite. Refer to MD-POL-100 Cybersecurity & Governance Policy, Appendix C for a list of related policies and standards.
Baseline	This standard has been developed using National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 Moderate Baseline[1] and State-specific organizationally defined parameters. Agencies may be required to deviate from this baseline when State statute, executive orders, or applicable regulations establish a conflicting requirement that precludes compliance.
Distribution	This document is approved for public distribution and may be shared with external stakeholders, partners, and regulatory bodies. It reflects the State’s commitment to transparency, compliance, and operational excellence. Unauthorized modifications or misrepresentation of this document are strictly prohibited.

[1] NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.

FOREWORD

Agencies that use Department of Information Technology DoIT-managed services automatically receive, or *inherit*, the compliance those services already meet, reducing duplicative work and accelerating their overall compliance efforts. These centrally governed services, such as hosting platforms, identity management, and network infrastructure, are built with robust control frameworks that automatically extend to participating agencies. By leveraging these offerings, agencies not only align with key operational and security standards but also benefit from pre-configured environments, continuous monitoring, and policy enforcement mechanisms maintained by DoIT. Agencies are encouraged to leverage these services to accelerate readiness, gain cost efficiency, simplify compliance efforts, and allow agencies to focus more fully on mission delivery, knowing that foundational requirements are already in place. Agencies should review the scope of each managed service to understand which standards are inherited and where additional agency-specific controls may still be required.

GUIDANCE AND ENFORCEABILITY

Throughout this document, informational call-out boxes are utilized to provide additional context or elaborate on key topics. While these boxes primarily serve an informational purpose, any directives or mandated actions contained within them are authoritative and carry the same enforceability as the core requirements of this document. For the purposes of this document, the term “shall” denotes a mandatory requirement. Terms such as “where feasible”, “encouraged”, or similar phrasing indicate recommended practices that reflect organizational preference but are not enforceable requirements at this time.

CHANGE RECORD

Version	Summary of Changes	Changed By	Date
1.0	Initial Publication	Miheer Khona	02/18/2026

STANDARDS

311 State Strategy

These standards establish a baseline of physical and environmental protections that each agency must implement to comply with State cybersecurity and privacy policies. Each agency shall designate specific personnel with IT responsibilities to ensure the effective implementation of these standards.

311-1 Develop Agency-Level Procedures (PE-1)

In alignment with this standard, develop and document agency-level physical and environmental protection procedures. Agencies must disseminate the procedures to agency personnel with information technology (IT) security responsibilities. Agencies must review, and if needed, update the procedures as deemed appropriate by the agency based on changes and risk at least every **3 years**. At a minimum, the procedures must address purpose, scope, roles and responsibilities, and guidelines.

311-2 Establish Physical Access Authorizations (PE-2)

Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides. Issue authorization credentials for facility access. Review the access list detailing authorized facility access by individuals at least **annually.** Remove individuals from the facility access list when access is no longer required.

311-3 Control Physical Access (PE-3)

Enforce physical access authorizations at entry and exit points to the facility where the system resides by:

- Verifying individual access authorizations before granting access to the facility;
- Controlling ingress and egress to the facility via physical access control systems/devices, or security guards;
- Where feasible, implement biometric authentication, smart card access, and real-time monitoring to detect unauthorized entry;
- Maintain physical access audit logs for all entry or exit points;
- Control access to areas within the facility designated as publicly accessible by implementing safeguards commensurate with assessed risk (e.g., guard stations, security cameras);
- Escort visitors and control visitor activity;
- Secure keys, combinations, and other physical access devices;

- Inventory physical access devices (e.g., keys, locks, card readers) at least annually; and
- Change combinations and keys when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

311-4 Control Access for Transmission (PE-4)

Control physical access to system distribution and transmission lines within organizational facilities using security controls that prevent accidental damage, disruption, and physical tampering. Protections are implemented to prevent eavesdropping or in-transit modification of unencrypted transmissions, stopping unauthorized individuals from altering the physical infrastructure.

Cable Protection
Cables should be routed through secure conduits, riser shafts, or locked telecom closets to prevent unauthorized contact and accidental damage. Access to these areas should be limited using keys or badge-controlled entry, surveillance systems, and escort policies for visitors or contractors. Tamper-evident seals, cable labeling, and periodic inspections can also help detect and deter physical tampering.

311-5 Control Access for Output Devices (PE-5)

Control physical access to output from information systems to prevent unauthorized individuals from obtaining the output.

311-6 Monitor Physical Access (PE-6)

Monitor physical access to the facility where the system resides to detect and respond to physical security incidents. Review physical access logs **monthly** and upon occurrence of any physical security incidents or suspicious activity (e.g., excessive access outside of normal work hours, repeated access to areas not normally accessed, out of sequence access). Where feasible, deploy surveillance systems, access logs, and anomaly detection for real-time threat response. Access logs must be collected and shared with DoIT Office of Security Management (OSM) to assist with data correlations and incident response activities.

PE-6(1): Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment. Closed-Circuit Television (CCTV) systems shall be installed and actively maintained at all perimeter ingress and egress points, as well as at access points to internal sensitive areas, including data centers, control rooms, and other mission-critical zones. Surveillance coverage must be continuous, tamper-resistant, and aligned with applicable privacy, security, and regulatory standards.

311-7 Maintain Visitor Access Records (PE-8)

Maintain visitor access records to the facility where the system resides for **3 years** or as required by the agency-specific records retention and disposition schedule, approved by the Maryland State Archives; Review visitor access records **monthly** and report anomalies in visitor access records to DoIT.

Include the following information in visitor access logs:

- Name and organization of person visiting;
- Signature of the visitor and form of identification;
- Date of access;
- Time of entry;
- Time of departure;
- Purpose of visit;
- Name and organization of person visited; and
- Inventory of assets entering and exiting the facility.

Visitors must be escorted at all times and must have their visitor ID badge visually displayed.

311-8 Protect Power Equipment and Cabling (PE-9)

Protect power equipment and power cabling for the system from damage and destruction.

311-9 Deploy an Emergency Shutoff Capability (PE-10)

Implement emergency shut-off capability for systems and system components within State facilities (e.g., data center, server rooms, mainframe rooms) in emergency situations. Place emergency shutoff switches or devices in designated locations to facilitate safe and easy access for authorized personnel. Protect emergency power shutoff mechanisms from unauthorized activation.

311-10 Establish Emergency Power Source (PE-11)

Provide and maintain an uninterruptible power supply (UPS) to facilitate an orderly shutdown of the system in the event of a primary power source loss. Where feasible, automate emergency response protocols with predefined access retractions.

311-11 Employ Emergency Lighting (PE-12)

Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility. Where feasible, integrate backup power and lighting systems into security monitoring frameworks.

311-12 Employ Fire Protection (PE-13)

Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

PE-13(1): Employ fire detection systems that activate automatically and notify designated officials and emergency responders in the event of a fire.

Fire Detection & Suppression

Selecting the appropriate fire suppression system for IT environments is critical to safeguarding equipment. Traditional, water-based sprinklers can cause irreparable damage to servers, network hardware, and storage arrays, so many organizations opt for clean agent systems like Halon, or inert gas blends like Argonite or Inergen. For small enclosures like server racks or telecom cabinets, spot suppression systems using aerosol or localized clean agents offer targeted defense.

311-13 Maintain Environmental Controls (PE-14)

Maintain temperature levels between 18–27 °C (64–80 °F) or as directed by equipment vendors.

311-14 Provide Water Damage Protection (PE-15)

Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

311-15 Control Delivery and Removal of Assets (PE-16)

Authorize and control system components entering and exiting the facility. Maintain records of the system components.

311-16 Identify Alternate Work Site (PE-17)

Determine and document alternate work sites allowed for use by employees; Employ and monitor effectiveness of security controls at alternate work sites. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

GUIDELINES

ID	Title	Description	Source
CSF Tools	Cyber Security Framework Tools	This website provides supplemental guidance for each security control listed in this document.	*csf.tools (LINK)*
NIST SP 800-12	An Introduction to Information Security	This document provides guidelines for physical and environmental security measures, associated with threats like fire, unauthorized access, and natural disasters.	*csf.tools (LINK)*
ISO 27001 Annex A.11	Physical & Environmental Security	This annex outlines necessary controls to safeguard and organization's physical assets and information processing facilities from various threats, including unauthorized access, environmental hazards, and malicious activities.	

DEFINITIONS

Each unique term used in this standard is defined in the **State of Maryland Cybersecurity & Privacy Glossary**.

COMPLIANCE CHECKLIST

ID	Standard	Compliance
311-1	**Develop Agency-Level Procedures (MP-1)**	☐ Yes ☐ No
311-2	**Establish Physical Access Authorizations (PE-2)**	☐ Yes ☐ No
311-3	**Control Physical Access (PE-3)**	☐ Yes ☐ No
311-4	**Control Access for Transmission (PE-4)**	☐ Yes ☐ No
311-5	**Control Access for Output Devices (PE-5)**	☐ Yes ☐ No
311-6	**Monitor Physical Access (PE-6)**	☐ Yes ☐ No
311-7	**Maintain Visitor Access Records (PE-8)**	☐ Yes ☐ No
311-8	**Protect Power Equipment and Cabling (PE-9)**	☐ Yes ☐ No
311-9	**Deploy Emergency Shutoff Capability (PE-10)**	☐ Yes ☐ No
311-10	**Establish Emergency Power Source (PE-11)**	☐ Yes ☐ No
311-11	**Employ Emergency Lighting (PE-12)**	☐ Yes ☐ No
311-12	**Employ Fire Protection (PE-13)**	☐ Yes ☐ No
311-13	**Maintain Environmental Controls (PE-14)**	☐ Yes ☐ No
311-14	**Provide Water Damage Protection (PE-15)**	☐ Yes ☐ No
311-15	**Control Delivery and Removal of Assets (PE-16)**	☐ Yes ☐ No
311-16	**Identify Alternate Work Site (PE-17)**	☐ Yes ☐ No

Note: When assessing the implementation and effectiveness of the security and privacy controls outlined in this standard, DoIT recommends the use of NIST SP 800-53A Rev. 5, to perform evaluations in a manner that is evidence-based, repeatable, and aligned with the system's documented security posture.