COMPLIANCE COMPONENT

DEFINITION

Name	Physical and Environmental Protection Controls
Description	Physical and Environmental Protection Controls refer to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment.
Rationale	Physical and Environmental Protection Controls are needed to protect the facility that houses system resources, the system resources themselves, and the facilities used to support their operation.
Benefits	Helps prevent: • Interruptions in information technology services • Physical damage • Loss of control over system integrity • Theft • Unauthorized access to, or disclosure of, information

ASSOCIATED ARCHITECTURE LEVELS

Specify the Domain Name	Security
Specify the Discipline Name	Operational Controls
Specify the Technology Area Name	Physical Security
Specify the Product Component Name	

COMPLIANCE COMPONENT TYPE

Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL

State the Guideline, Standard or Legislation	An agency's physical and environmental protection controls should address all of the following topics: 1) Physical and Environmental Protection Policy and Procedures **-** This control addresses the establishment of physical and environmental policy and procedures for the agency. 2) Physical Access Authorizations - Develops, approves, maintains and reviews a list of individuals with authorized access to the facility where the information system resides. 3) Physical Access Control – The enforcement of physical access authorizations. 4) Access Control for Transmission Medium - Physical security safeguards applied to information system distribution and transmission lines that help to prevent accidental damage, disruption, and physical tampering. These safeguards include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

	5) Access Control for Output Devices - The agency should control physical access to information system output devices to prevent unauthorized individuals from obtaining the output. 6) Monitoring Physical Access – The agency should monitor physical access, reviews physical access logs, and coordinates results of reviews and investigations for the facility where the information system resides. 7) Visitor Access Records – The agency should maintain and review visitor access records. 8) Power Equipment and Cabling - The agency should protect power equipment and power cabling for the information system from damage and destruction. 9) Emergency Shutoff – The agency should provide the capability of shutting off power to the information system, place emergency shutoff switches or devices to facilitate safe and easy access for personnel, and protect emergency power shutoff capability from unauthorized activation. 10) Emergency Power - The agency should provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system or a transition of the information system to long-term alternate power in the event of a primary power source loss. 11) Emergency Lighting – The agency should employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption, which covers emergency exits and evacuation routes within the facility. 12) Fire Protection - The agency should employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source. 13) Temperature and Humidity Controls – The agency should maintain and monitor temperature and humidity controls within the facility where the information system resides. 14) Water Damage Protection - The agency should protect the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, work properly, and are known to key personnel. 15) Delivery and Removal - The agency should authorize, monitor, and control any information system components entering and exiting the facility, and maintains records of those items. 16) Alternate Work Site – The agency should apply appropriate security controls at alternate work sites. These alternative work sites should also provide a means for employees to communicate with information security personnel in case of security incidents or problems. 17) Location of Information System Components - The agency should position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. 18) Information Leakage - The agency should protect the information system from information leakage due to electromagnetic signals emanations. 19) Asset Monitoring and Tracking – The agency should employ asset location technologies to track and monitor the location and movement of assets.
Document Source Reference #	NIST (SP) 800-12 Rev. 1, An Introduction to Information Security (June 2017) NIST (SP) 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations (Jan 2015)

Compliance Sources

Name	National Institute of Standards and Technology (NIST), Computer Security	*Website*	http://csrc.nist.gov/

	Resource Center (CSRC)		
Contact Information	inquiries@nist.gov		
Name		*Website*	
Contact Information			

KEYWORDS

List Keywords	Storage, power, utilities, fire, flood, natural disaster, generator, UPS, keycard, Sonitrol, biometric, access control.

COMPONENT CLASSIFICATION

Provide the Classification	□ *Emerging*	☒ *Current*	□ *Twilight*	□ *Sunset*
Sunset Date				

COMPONENT SUB-CLASSIFICATION

Sub-Classification	Date	Additional Sub-Classification Information
□ *Technology Watch*		
□ *Variance*		
□ *Conditional Use*		

Rationale for Component Classification

Document the Rationale for Component Classification	

Migration Strategy

Document the Migration Strategy	It is understood that not all buildings currently occupied by state agencies are able to meet the requirements of this Compliance Component. This document should be used when considering relocation or occupancy of future sites.

Impact Position Statement

Document the Position Statement on Impact	

CURRENT STATUS

Provide the Current Status	□ *In Development*	□ *Under Review*	☒ *Approved*	□ *Rejected*

AUDIT TRAIL

Creation Date	03/01/2007	*Date Approved / Rejected*	03/23/2007
Reason for Rejection			
Last Date Reviewed	10/18/2018	*Last Date Updated*	10/18/2018
Reason for Update			