COMPLIANCE COMPONENT

DEFINITION	
Name	Physical and Environmental Security Controls
Description	Physical and Environmental Security Controls is the application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information.
Rationale	Physical and Environmental Security Controls are implemented 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 • Unauthorized disclosure of information • Loss of control over system integrity • Theft • Unauthorized access to 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	The responsibility for the physical and environmental security program should be formally assigned. An agency's physical and environmental security program must address the following eight topics. **Physical Access Controls** • Physical access controls must address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media, and any other elements required for the system's operation. • Control access to critical areas facilities with conventional or electronic door locks; supervision by guards or receptionists over movement of people and materials; administrative procedures (sign-in logs, identification cards or badges, property passes and shipping/receiving forms); and other policy or regulations.

- Visitors should be properly controlled and escorted
- A visitor's log should be kept and reviewed regularly

- It is important to review the effectiveness of physical access controls in each area, both during normal business hours and at other times -- particularly when an area may be unoccupied.

- Examples of best practices for physical access controls include:
  - Signs at the door(s) marking the room as restricted access and prohibiting food, drink, and smoking in the computer room.
  - Automatic authentication method at the entrance to the room (such as a badge reader).
  - Only two doors to a computer room (a room with one door in a computer room without windows is probably a violation of fire code as there must be two egress points).
  - Computer rooms should be monitored by CCTV cameras.
  - Each computer room should have redundant access to power, cooling, and networks.

Environmental Controls

- There should be at least an 18" access floor to provide for air flow and cable management.
- Computer rooms should have air filtration
- Computer rooms should have high ceilings to allow for heat dispersal
- Each computer room should have temperature between 55 and 75 degrees Fahrenheit and a humidity of between 20 and 80 percent. Environmental sensors should log the temperature and humidity of the room

Fire Safety Factors

- Fires are a unique threat because of the potential for damage to hardware and data, the risk to human life, and the pervasiveness of the damage. Smoke, corrosive gases and high humidity from fire, anywhere in the building, can damage systems throughout the entire building. Consequently, it is important to evaluate the fire safety of buildings that house systems
- Agencies must provide fire detection and extinguishment as required by local authorities
- Agencies should train personnel in fire suppression
- There should be an oxygen depleting agent or other total flooding agent solution in place in each computer room
- There must be fire extinguishers located in each computer room
- There must be emergency power off switches inside each computer room
- There should be respirators in computer rooms
- There must not be wet pipe sprinkler systems installed in computer rooms

Failure of Supporting Utilities

- Computer systems and the people who operate them need to have a reasonably well-controlled operating environment. Consequently, failures of electric power, heating and air-conditioning systems, water, sewage, and other utilities will usually cause a service interruption and may

damage hardware

- Agencies should ensure that these utilities, including their associated elements, function properly
- There must be battery backup power onsite with sufficient duration to switch over to a continuous power generation
    - If there is continuous power generation on site then 24 hours of fuel should be available on site
    - A contract should be in place to obtain up to a week of fuel to the facility
- If there is no continuous power generation backup then there should be 24 hours of battery power available

Structural Collapse

- Agencies must be aware that a building may be subjected to a load greater than it can support
- Most commonly this is a result of an earthquake, a snow load on the roof beyond design criteria, an explosion that displaces or cuts structural members, or a fire that weakens structural members

Plumbing Leaks

- While plumbing leaks do not occur every day, they can be seriously disruptive
- An agency must know the location of plumbing lines that might endanger system hardware and take steps to reduce risk such as:
    - Moving hardware
    - Relocating plumbing lines
    - Identifying shutoff valves
    - Provide water damage equipment such as mops, buckets, towels, wet-dry vacuums, fans, etc.
    - Flood-control equipment such as pumps, tarpaulins, sand bags, etc.

Interception of Data

- Depending on the type of data a system processes, there may be a significant risk if the data is intercepted
- Agencies must be aware that there are three methods of data interception:
    - Direct observation
    - Interception of data transmission
    - Electromagnetic interception

For additional information regarding handling an incident, please see the Incident Response Reporting CC.

Mobile and Portable Systems

- The analysis and management of risk usually has to be modified if a system is installed in a vehicle or is portable, such as a laptop computer
- The system in a vehicle will share the risks of the vehicle, including accidents and theft, as well as regional and local risks
- Agencies must physically secure storage of laptop computers or other mobile devices when they are not in use

Document Source Reference #	NIST (SP) 800-14 Generally Accepted Principles and Practices for Securing Information Technology and SANS Institute 2003 Best Practices		
Compliance Sources			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
Name		*Website*	
Contact Information			
KEYWORDS			
List Keywords	Storage, power, utilities, fire, flood, natural disaster, generator, UPS, keycard, Sonitrol, biometrics.		
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		*Last Date Updated*	
Reason for Update			