**Physical Environmental Protection Policy Template**

# PURPOSE

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure that “YOUR AGENCY NAME” develops, disseminates, and updates the Physical and Environmental Protection Policy. This policy and procedure establishes the minimum requirements for the Physical and Environmental Protection Policy.

This policy is intended to meet the control requirements outlined in SEC501, Section 8.11 Physical and Environmental Protection Family, Controls PE-1 through PE-19 as well as additional Commonwealth of Virginia controls.

# SCOPE

All “YOUR AGENCY NAME” employees (classified, hourly, or business partners) as well as all “YOUR AGENCY NAME” systems

# ACRONYMS

CIO: Chief Information Officer

COV: Commonwealth of Virginia

CSRM: Commonwealth Security and Risk Management

FTI Federal Tax Information

ISO: Information Security Officer

IT: Information Technology

ITRM: Information Technology Resource Management

SEC501: Information Security Standard 501

UPS: Uninterruptible Power Supply

“YOUR AGENCY NAME”: “YOUR AGENCY NAME”

# DEFINITIONS

[See COV ITRM Glossary](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/EA_PSG_update_011510/ITRMGlossary_011510.pdf)

# BACKGROUND

The Physical and Environmental Protection Policy at “YOUR AGENCY NAME” is intended to facilitate the effective implementation of the processes necessary to meet the physical and environmental protection requirements as stipulated by the COV ITRM Security Standard SEC501 and security best practices. This policy directs that “YOUR AGENCY NAME” meet these requirements for all IT systems.

# ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibilities as described in the Statement of Policy section. The following Roles and Responsibility Matrix describe 4 activities:

1. Responsible (R) – Person working on activity
2. Accountable (A) – Person with decision authority and one who delegates the work
3. Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
4. Informed (I) – Person who needs to know of decision or action

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Roles** | Data Owner | System Owner | System Admin | Information Security Officer |
| **Tasks** |   |   |   |   |
| Identify whether it assets may be removed from premises. |  |  I | I | A/R |
| Design safeguards to protect against human, natural, and environmental threats. |  | I | I | A/R |
| Restrict access to “YOUR AGENCY NAME” buildings to authorized personnel. |  |  | R | A |
| Maintain a list of personnel with authorized access. |  |  | R | A |
| Issue authorization credentials. |  |  | R | A |
| Review and approve access list and authorization credentials. |  |  |  | A/R |
| Disable or remove access rights. |  |  | R | A |
| Enforce and verify physical access authorizations using physical access devices, |  |  |  | A/R |
| Inventory physical access devices. |  |  | R | A |
| Control physical access to information system output devices. |  |  | R | A |
| Monitor physical access and respond to detected physical security incidents. |  |  | R | A |
| Control physical access to facilities by authenticating and escorting visitors. |  |  | R | A |
| Maintain access records for visitors and authorized individuals. |  |  | R | A |
| Inspect and protect power equipment and cabling. |  |  | R | A |
| Provide emergency shutoff switches. |  |  |  | A/R |
| Provide and test ups for critical devices. |  |  | R | A |
| Employ and maintain a fire suppression and detections system. |  |  | R | A |
| Maintain temperature and humidity levels. |  |  | R | A |
| Position information system components to minimize potential damage from physical and environmental hazards. |  |  | R | A |

# STATEMENT OF POLICY

In accordance with SEC501, PE-1 through PE-19, “YOUR AGENCY NAME” shall establish a set of requirements that defines the minimum level of physical and environmental security for all “YOUR AGENCY NAME” facilities to safeguard information resources.

1. **PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES**
	1. The ISO or designee shall:
		1. Identify whether IT assets may be removed from premises that house IT systems and data, and if so, identify the controls over such removal.
		2. Design safeguards, commensurate with risk, to protect against human, natural, and environmental threats.
		3. Communicate changes, results, breaches, as required, to stakeholders with a need to know.
2. **PHYSICAL ACCESS AUTHORIZATIONS**
	1. The ISO or designee shall:
		1. Restrict access to “YOUR AGENCY NAME” buildings, rooms, work areas, spaces, and structures housing information systems, equipment, and data to authorized personnel;
		2. Develop and keep current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
		3. Issue authorization credentials (e.g., badges, identification cards, and smart cards);
			1. The level of access provided to each individual must not exceed the level of access required to complete the individual’s job responsibilities.
				1. The level of access must be reviewed and approved
			2. Keys, badges, access cards, and combinations must be issued to only those personnel who require access.
			3. Authorizations and requirements for access must be coordinated with facility and personnel security managers, as required or needed.
		4. Review and approve the access list and authorization credentials quarterly, removing from the access list personnel no longer requiring access;
		5. Temporarily disable physical access rights when personnel do not need such access for a prolonged period in excess of 30 days because they are not working due to leave, disability or other authorized purpose;
		6. Disable physical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes; and
		7. Promptly remove access rights for terminated personnel or for personnel no longer requiring access.
3. **PHYSICAL ACCESS CONTROL**
	1. The ISO or designee shall:
		1. Enforce physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides;
			1. Those areas within the facilities officially designated as publically accessible may be excluded from this requirement.
		2. Verify individual access authorizations before granting access to the facility;
		3. Ensure that the authorization credential (e.g., badges, identification cards, and smart cards) is worn on the person, above the waist, and is visible at all times;
		4. Control entry to the facility containing the information system using physical access devices (e.g., keys, locks, combinations, card readers) and/or guards (e.g., professional physical security staff, administrative staff, information system users);
		5. Control access to areas officially designated as publicly accessible in accordance with the organization’s assessment of risk;
		6. Secure keys, combinations, and other physical access devices;
			1. Stringent key and combination controls must be implemented at the facilities or designated areas within facilities, as applicable to ensure physical access protections.
			2. Combinations and keys must be changed immediately for reasons such as:
				1. Keys are lost.
				2. Combinations are compromised.
				3. Individuals are transferred, terminated, or no longer need access.
				4. There is a theft or security violation in the area being protected.
		7. Inventory physical access devices at least once a quarter;
		8. Enforce physical access authorizations to the information system independent of the physical access controls for the facility;
			1. This requirement applies to server rooms, media storage areas, communications centers, or any other areas within a “YOUR AGENCY NAME” facility containing large concentrations of information system components.
			2. All visitors to the CESC/SWESC data centers are accompanied by an FTI-authorized escort at all times. Any single escort cannot be assigned more than four (4) individuals to escort per event.
		9. Safeguard IT systems and data residing in static facilities (such as buildings), mobile facilities (such as computers mounted in vehicles), and portable facilities (such as mobile command centers).
4. **ACCESS CONTROL FOR OUTPUT DEVICES**
	1. The ISO or designee must control physical access to information system output devices, such as monitors, printers, and audio devices, to prevent unauthorized individuals from obtaining the output.
		1. Methods to protect display devices include repositioning the monitor and/or using a monitor filter.
5. **MONITORING PHYSICAL ACCESS**
	1. The ISO or designee must:
		1. Monitor physical access to the information system to detect and respond to physical security incidents;
		2. Review physical access logs at least once every 60 days;
		3. Investigate apparent security violations or suspicious physical access activities. Investigations and results of reviews must be coordinated with “YOUR AGENCY NAME”’s incident response capability;
			1. Remedial actions identified as a result of investigations must be developed and implemented.
		4. Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities must be part of “YOUR AGENCY NAME”’s incident response capability; and
			1. Individuals who have physical protection response responsibilities must be identified in writing.
			2. Operational procedures must be developed to document how these individuals shall respond to physical access incidents.
		5. Install and monitor real-time physical intrusion alarms and surveillance equipment.
6. **VISITOR CONTROL**
	1. The ISO or designee shall control physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.
		1. Individuals (to include organizational employees, contract personnel, and others) with permanent authorization credentials for the facility are not considered visitors.
	2. The ISO shall require that visitors be escorted and that visitor activity is monitored, when required.
		1. Visitors requiring access to sensitive information system areas must be escorted.
		2. All visitors shall sign a visitor log.
	3. The ISO shall require that visitors show a valid form of picture identification such as: current driver’s license, passport or employer ID badge.
7. **ACCESS RECORDS**
	1. The ISO shall require that:
		1. Visitor access records to the facility are maintained where the information system resides (except for those areas within the facility officially designated as publicly accessible); and
			1. The visitor access record must address the following components:
				1. Name and organization of the person visiting.
				2. Signature of the visitor.
				3. Form(s) of identification.
				4. Date of access.
				5. Time of entry and departure.
				6. Purpose of visit.
				7. Name and organization of person visited.
				8. Reviews visitor access records at least once every 60-days.
		2. A record of all physical access, both visitor and authorized individuals must be maintained.
			1. Records will be reviewed at least every 60 days.
8. **POWER EQUIPMENT AND POWER CABLING**
	1. The ISO or designee shall require that power equipment and power cabling for the information system is protected from damage and destruction.
		1. Power cabling must be inspected on an annual basis for the following:
			1. Power cables under raised floors and in drop ceilings must be inspected for fraying or other wear, such as damage from water or pest infestation.
			2. Facilities with hangers and trays that support power cables must be inspected for stability.
		2. The results of the inspection must be documented to include the following:
			1. Date(s) of inspection.
			2. Person(s) conducting inspection(s).
			3. Location(s) inspected.
			4. Component(s) inspected.
			5. Inspection results include, but not limited to Escalation Required & Remedial Actions Taken and Final Inspection.
9. **EMERGENCY SHUTOFF**

Note: This control applies to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.

* 1. The ISO or designee shall require:
		1. The capability of shutting off power to the information system or individual system components in emergency situations must be provided;
		2. Emergency shutoff switches or devices must be place in organization-defined location by information system or system component to facilitate safe and easy access for personnel; and
			1. The locations for emergency power shutoffs must be documented.
			2. All necessary personnel must be informed of the emergency shutoff locations and they must be trained to operate the safely.
			3. Emergency procedures must be readily available to relevant personnel.
			4. Emergency shutoff switches must be located in a visible location and clearly labeled.
		3. The emergency power shutoff capability must be protected from unauthorized activation.
1. **EMERGENCY POWER**
	1. The ISO or designee shall:
		1. Ensure a short-term uninterruptible power supply (UPS) is installed to facilitate an orderly shutdown of the information system in the event of a primary power source loss.
			1. The UPS must be tested by certified technician at least once a year or when any material change is made to the UPS.
			2. Servers and critical hardware devices must be protected by a UPS, installed either centrally or locally.
2. **FIRE PROTECTION**
	1. The ISO or designee shall employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.
		1. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.
		2. Fire extinguishers must be checked on an annual basis and the inspection date must be documented on the extinguisher.
		3. All server/computer rooms or data centers must have at least one hand-held fire extinguisher that it easily accessible.
		4. Personnel must be trained on how to use a fire extinguisher and must receive annual refresher training.
		5. All fire protection resources must be tested on an annual basis in accordance with local or state fire regulations to ensure they can be successfully activated in the event of a fire.
3. **TEMPERATURE AND HUMIDITY CONTROLS**
	1. The ISO or designee shall ensure that:
		1. Temperature and humidity levels within the facility, where the information system resides. are maintained at organization-defined acceptable levels.
		2. Temperature and humidity levels are monitored and recorded on a daily basis.
		3. Remedial corrective actions are coordinated and logged as necessary.
4. **LOCATION OF INFORMATION SYSTEM COMPONENTS**
	1. The ISO shall require that:
		1. Information system components must be positioned within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.
			1. Examples of minimizing potential damage by careful positioning include these:
				1. In an earthquake zone, an unanchored/untethered storage cabinet should not be placed next to critical equipment, lest it fall over and damage the equipment.
				2. If water pipes are running overhead, then cabling or equipment should not be placed underneath the pipes.

Note: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and electromagnetic radiation.

* + 1. The location or site of the facility must be considered with regard to physical and environmental hazards.
		2. The location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to the information system and therefore, increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones) must be considered.
		3. The location or site of the facility where the information system resides must be planned with regard to physical and environmental hazards.
		4. For existing facilities, the physical and environmental hazards must be considered in the risk mitigation strategy for the information system.

# ASSOCIATED

**PROCEDURE** “YOUR AGENCY NAME” Information Security Program Policy

**AUTHORITY**

**REFERENCE** [*Code of Virginia, §2.2-2005 et seq.*](http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2005)

(Powers and duties of the Chief Information Officer “CIO”““YOUR AGENCY NAME””)

**OTHER**

**REFERENCE** [ITRM Information Security Policy (SEC519)](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Security_Policy_519_00_Final_0709.pdf)

 [ITRM Information Security Standard (SEC501)](http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501_06_07012011.pdf)

| Version History |
| --- |
| Version | Date | Change Summary  |
| 1 | 07/01/2014 | Original |
| 2 | 0716/2014 | Additions made to **C. PHYSICAL ACCESS CONTROL**, items 1 c., and 1.i. ii. to address FTI requirements. |
| 3 | 12/21/2021 | Formatting changes |