**Gap Analysis to Support the Implementation of the South Carolina**

**Physical & Environmental Security Policy**

The below Gap Analysis is developed based on the feedback provided by the policy implementation team of the (SC State Agency). The table outlines the policy requirements (procedures, standards and policies which may/may not be implemented), relevant questions to address and identify gaps in the Agency’s environment.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Policy Requirement** | **Questions** asset inventory? | **YES , NO or N/A** | **Gap** | **Comments** |
| **InfoSec Policy has been reviewed and approved by the key stakeholders.** | **Has the InfoSec Policy been reviewed and approved by the key stakeholders?** |  |  |  |
| **InfoSec Policy has been approved and received sign off by the authorized executives.** | **Has the policy been approved and received sign off by the authorized executive?** |  |  |  |
| **The policy has been socialized across the Agency for personnel awareness.** | **Has the policy been shared with all personnel across-Agency?** |  |  |  |
| Document and implement Physical and Environmental Protection Policy and associated controls | Does your Agency have a documented Physical and Environmental Security Policy? |  |  |  |
| Develop Physical Access Authorizations processes | Has your Agency established a list of personnel with authorized access to the facility where the information systems are physically located? (e.g., data center) |  |  |  |
| Does your Agency have a process to request, review and approve new user access to facilities (e.g. data center)? |  |  |  |
| If so, is the documentation maintained for the above request process? |  |  |  |
| Has the Agency identified the appropriate personnel who is/are responsible for reviewing and maintaining access to the facilities? |  |  |  |
| Does the Agency have a process to remove physical access to facilities (e.g. data center) in a timely manner (e.g. within 24-72 hours of the employee being terminated or no longer needing access per current job responsibilities)? |  |  |  |
| If so, is the documentation maintained for the removal of facilities access outlined in the above process? |  |  |  |
| Does your Agency have a process to maintain or periodically review the list of personnel with access to facilities? |  |  |  |
| If so, is the documentation maintained and any change of access requested during the reviewed followed through with to complete the review process (e.g. if a user no longer requires access and is identified as such during the review, their access is revoked and acknowledgement is made that the change was followed through to completion)? |  |  |  |
| Develop Physical Access Control processes | Has the Agency implemented physical access controls to restrict entry to / exit from sensitive facilities (e.g., data centers)?  For example, keycards, keypin locks (with logging capabilities). |  |  |  |
| Does the Agency have physical access audit logs for the sensitive facilities’ entry / exit points?  Keycard systems retain access logs automatically; Agencies should configure logs to help ensure these are in compliance with policies and procedures, such as level of detail and retention. If electronic logs are not available, consider implementing manual logs to be maintained by a designated responsible. |  |  |  |
| Has the Agency implemented mechanisms to monitor for unauthorized access to sensitive facilities on a 24/7 basis?  For example, Agencies may employ security guards or alarms to monitor physical entry / exit points. Also, some keycard systems have alarm and automated notification capabilities. |  |  |  |
| Does the Agency conduct security assessments at least annually on sensitive facilities to check for unauthorized extraction or removal of information system components?  For example, Agencies may implement a process to perform physical walkthroughs of sensitive facilities on a periodic basis, and document and report on results. |  |  |  |
| If physical locks are in use to control physical access, does the Agency change combination locks and keys at defined intervals? |  |  |  |
| Has the Agency implemented a process to change combinations if these are compromised or keys if these are lost? |  |  |  |
| Does the Agency change keys and combinations after employees are transferred or terminated? |  |  |  |
| Establish Access Control Measures for Data / Information Transmission Medium | Has the Agency implemented physical security access controls to facilities where information system distribution and transmission lines are located? |  |  |  |
| Establish Access Control Measures for Data Output Devices | Does the Agency place output devices (e.g., printers, scanners, copiers, etc.) in secured areas and in locations that can be monitored by authorized personnel? |  |  |  |
| Does the Agency control access to physical output devices (e.g., printers, copiers, scanners, facsimile machines, etc.) to prevent unauthorized individuals from obtaining sensitive data? |  |  |  |
| Establish a process to Monitor Physical Access | Does the have a process to collect and record physical access logs to the data center? |  |  |  |
| Does the Agency review physical access logs on a defined schedule (established by the Agency)? |  |  |  |
| Does the Agency review physical access logs upon the occurrence of a security incident? |  |  |  |
| Where applicable, has the Agency established a process to report on security violations and incidents? |  |  |  |
| Establish Visitor Access Control | Has the Agency established a process to escort visitors while on sensitive facilities?  The visitor escorting process should include escorting visitors from time of arrival and upon exit from the facility. |  |  |  |
| Does the Agency maintain visitor access records (i.e., logs to data center(s) and other sensitive facilities for a minimum of 1 year?  Visitor logs should include enough details to identify visitors (e.g., first and last name), understand the purpose of the visit, Agency contact, date and time, among other details. Also, logs should be filled out by Agency personnel escorting visitors, or by Security guards. |  |  |  |
| Establish Equipment Delivery and Removal processes | Has the Agency established a process to monitor (e.g. supervise the equipment that enters/exists the data center) and control assets / equipment entering and exiting the data center(s)? |  |  |  |
| Has the Agency established a process to approve the delivery and removal of equipment in the data center(s)? |  |  |  |
| Does the Agency maintain records of assets / equipment entering or leaving data center(s)? |  |  |  |
| Establish process for the accurate and secure placement of Power Equipment and Cabling | Does the Agency place power equipment and cabling in safe locations (e.g. generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites? |  |  |  |
| Establish Emergency Shutoff Procedures | Does the Agency have the capability of shutting off power to data center(s) during an incident (e.g., flash floods, hurricane events, etc.)? |  |  |  |
| Does the Agency place emergency shutoff switches or devices at locations that are safe and easily accessible by authorized Agency personnel during an incident? |  |  |  |
| Has the Agency installed physical (e.g., physical locks) or logical (e.g., fingerprint scan) controls to protect emergency power shutoff capability (i.e., switches) from unauthorized activation?  While this question seems in contradiction to the above, the purpose of this policy requirement is to prevent the emergency power shutoff from being accessed by any employee. For the data center, there should be physical and logical controls implemented to restrict access to authorized employees only. For those authorized employees, the emergency shutoff switch should be in a location that is safe and accessible, but again, there should be physical and logical controls established before it can be accessed. |  |  |  |
| Establish Emergency Power source for the Data Center(s) | Has the Agency established an UPS (uninterrupted power supply) to support the start of a long-term, alternative power supply source (e.g., industrial grade generator and dedicated fuel source) in the event of a primary power source failure? |  |  |  |
| Establish Fire Suppression processes and associated mechanisms | Has the Agency established and maintained fire detection and suppression (e.g., FM-200, a waterless fire suppressant) systems? |  |  |  |
| Does the Agency’s fire detection and suppression system receive power from an independent power source? |  |  |  |
| Is the Agency’s fire detection and suppression system capable of automatically notifying emergency personnel in the event of a fire hazard? |  |  |  |
| Has the Agency identified emergency responders (i.e., county paramedics, law and order personnel, other emergency responders) in the event of a fire hazard on the premises? |  |  |  |
| Does the fire suppression system installed on the premises have the required automation capabilities (automatic power-on, alarm system, etc.) if the data center is not staffed on a continuous basis? |  |  |  |
| Establish Temperature and Humidity Controls for Data Center(s) | Does the Agency employ automated temperature and humidity controls (e.g., thermostat cut-off based HVAC systems), in the data center(s) to prevent fluctuations which could potentially be harmful to processing equipment (i.e., servers and other optical storage devices)? |  |  |  |
| Has the Agency installed a temperature and humidity monitoring system which has an alarm / notification capability to warn authorized Agency personnel of potential / impending harm to network and processing equipment? |  |  |  |
| Establish Data Center Water Damage Protection measures | Has the Agency installed raised platforms to house data center equipment (i.e., servers and network switches, routers) and protect them from potential damage in the event of a water leakage? |  |  |  |
| Establish procedures for Media Sanitization | Does the Agency sanitize removable digital and non-digital media prior to disposal, in accordance with federal and Agency standards and policies? |  |  |  |
| Does the Agency sanitize removable digital and non-digital media prior to release outside of the Agency, in accordance with federal and Agency standards and policies? |  |  |  |
| Does the Agency sanitize removable digital and non-digital media prior to release for reuse, in accordance with federal and Agency standards and policies? |  |  |  |
| Has the Agency established mechanisms to dispose digital media and data storage devices? |  |  |  |
| Has the Agency established a procedure to clean and dispose computers, hard drives and fax/printer/scanner devices? |  |  |  |
| Are all sanitization activities (e.g., cleansing and disposal of laptops) documented, tracked and maintained within the Agency? |  |  |  |