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

**Threat and Vulnerability Management 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?** |  |  |  |
| Develop a Vulnerability Assessment Policy | Has your Agency developed a Vulnerability Assessment Policy? |  |  |  |
| Establish processes for Vulnerability Scanning | Does your Agency scan for vulnerabilities within information systems and hosted applications at least annually? |  |  |  |
| Does your Agency have a process to report new vulnerabilities identified through vulnerability scans? |  |  |  |
| Are processes established to remediate identified vulnerabilities in accordance with the results of the vulnerability assessment performed? |  |  |  |
| Are controls established to limit privileged access (e.g. access to make configuration or access changes) to vulnerability scanning tools and the resulting reports? |  |  |  |
| Does your Agency perform security controls assessments (e.g a security controls assessment determines whether security controls in an information system are operating as intended)? |  |  |  |
| Are processes established to remediate identified vulnerabilities in accordance with the results of the security controls assessment performed? |  |  |  |
| Has the Agency determined a risk ranking strategy for identified vulnerabilities? |  |  |  |
| Develop a Penetration Testing schedule | Does your Agency conduct penetration testing exercises on an annual basis (internal resources or third-party teams are acceptable)? |  |  |  |
| Develop an Incident Response Policy and associated procedures | Has the Agency developed an incident response policy? |  |  |  |
| If so, does it address the following elements: * Scope
* Roles
* Responsibilities
* Internal coordination efforts
* Compliance
 |  |  |  |
| Has your Agency established documented procedures to assist in the implementation of the incident response policy?(Note: Typically incident response procedures could be inclusion of the following:* Nominating an incident response team (typical team comprises of IT personnel, legal representative, public relations, officer, departmental/executive management depending on the scale of incident)
* Initial assessment of the incident
* Developing initial response to the incident
* Collecting forensic evidence
* Implementing temporary fix
* Communications (i.e., internal and external)
* Implementing permanent fix
* Determining financial impact on operations)
 |  |  |  |
| Does your Agency review and update the incident response policy and the associated procedures on an annual basis? |  |  |  |
| Develop an Incident Response Plan | Has your Agency developed an Incident Response Plan to establish a plan of action to implement incident response capabilities? |  |  |  |
| Does your Agency document the requirements of the organization, including: * Mission
* Size
* Structure
* Functions?
 |  |  |  |
| Does your Agency define the information security incidents that are required to be reported? |  |  |  |
| Has the Agency determined to whom the report will be shared and reported? |  |  |  |
| Does your Agency establish metrics (e.g. benchmarking) to test the effectiveness of the incident response plan? |  |  |  |
| Does your Agency define technology and personnel resources to effectively support incident response capabilities? |  |  |  |
| Does your Agency review and update the incident response plan annually? |  |  |  |
| Develop an Incident Handling process | Has your Agency implemented a formal process to handle security incidents to include: * preparation (e.g., nominating a team of key individuals),
* detection (e.g., receiving initial communication of the incident) and analysis (e.g., analyzing the nature of the incident),
* containment (e.g., formalizing steps to limit the effects of the incident on operations),
* eradication (e.g., formalizing steps to eliminate the identified incident), and
* recovery (e.g., bringing operations back to last known state)?
 |  |  |  |
| Has your Agency implemented tools or mechanisms (e.g., intrusion detection and prevention systems, firewalls, etc.) to respond to security incidents? |  |  |  |
| Develop Incident Monitoring and Reporting | Does your Agency have an incident response team? |  |  |  |
| Has your Agency established processes and required (detection) tools (e.g., Intrusion Detection Systems (ISDs) to record information security incidents occurring in external and internal information systems? |  |  |  |
| Does your Agency have a process in place for personnel to report information security incidents? |  |  |  |
| Has the Agency determined to whom the incidents will be shared and reported (e.g. incident response team and/or Agency management)? |  |  |  |
| Develop an Information System Monitoring process | Does your Agency monitor information systems to detect attacks or potential attacks? |  |  |  |
| If so, does the monitoring include unauthorized network or local / remote connections? |  |  |  |
| Has your Agency determined the team or individual responsible for monitoring information system attacks? |  |  |  |
| Has your Agency deployed monitoring devices within the information technology environment to collect information on security events? |  |  |  |
| Does your Agency protect the information obtained from intrusion-monitoring tools against unauthorized access, modification, and deletion? |  |  |  |
| Does your Agency monitor inbound and outbound communications traffic from the information systems for unusual or unauthorized activities (e.g., access)? |  |  |  |
| In times where this is increased risk to operations, individuals or assets within the Agency, is there a process or procedure established to heighten the level of security monitoring? |  |  |  |
| Develop an Incident Response Training Program | Does your Agency provide incident response training to employees appointed in the incident response roles or responsibilities? |  |  |  |
| If so, does this training occur within one (1) month of an individual starting incident response responsibilities?  |  |  |  |
| Does your Agency provide incident response training to employees upon major changes to the information systems and / or changes to the incident response plan? |  |  |  |
| Develop an Incident Response Testing Program | Does your Agency test incident response capabilities on a yearly basis? |  |  |  |
| If so, are the results of the test documented? |  |  |  |
| Do the results of the test drive updates to the incident response processes and procedures? |  |  |  |
| Develop processes to protect against Malicious Code | Does your Agency employ malicious code protection mechanisms to detect and eradicate such code? |  |  |  |
| If so, are malicious code protection mechanisms deployed on information systems input and output points? |  |  |  |
| Has your Agency implemented a process to update malicious code protection mechanisms when such updates are available? |  |  |  |
| Does your Agency configure malicious code protection mechanisms such that periodic scans are performed at specific time intervals? |  |  |  |
| Does your Agency have a process to block malicious code? |  |  |  |
| If so, it is programmed to send alerts to the information system administrator (or other Agency personnel) such that required actions could be initiated in response to the malicious code detection? |  |  |  |
| Establish a Flaw Remediation processes | Has your Agency developed a process to identify and remediate information system flaws? |  |  |  |
| Develop Patch release and management processes | Has your Agency established a process to test software which could analyze software and firmware updated before these are deployed on information systems? |  |  |  |
| Has your Agency installed updated and stable releases of available security and firmware patches? |  |  |  |
| Has the agency established a process to identify when latest stable, applicable patches are released by vendors? |  |  |  |
| Establish a Patch Cycle and Testing Process  | Has your Agency established a patch cycle which would monitor the application of patches and updates to systems? |  |  |  |
| Has your Agency established a process to test the validity of the path source? |  |  |  |
| Does your Agency ensure test environment for a seamless patch roll out? |  |  |  |