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

**Master 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 and communicate the Information Security Plan within the Agency | Has your Agency developed and communicated an information security plan outlining:* Security requirements (i.e., physical and logical);
* Security management controls (i.e., provisioning and de-provisioning exercises); and
* Common controls (i.e., access request forms, approval processes, etc.) to meet the security requirements?
 |  |  |  |
| If so, does the Agency’s security plan identify and assign security program roles (e.g., Chief Information Security Officer (CISO)), and responsibilities and management commitment (i.e., scheduled progress review meetings)? |  |  |  |
| Does the Agency’s security plan ensure coordination among the Agency’s business units (e.g., IT department and HR department) responsible for different aspects of information security (i.e., technical, physical, personnel, etc.)? |  |  |  |
| Has your Agency’s security plan been approved by the senior management (i.e., General Counsel (if applicable) and Agency Director)? |  |  |  |
| Does your Agency review the security plan at least on an annual basis and make modifications, if necessary? |  |  |  |
| Does the Agency update the security plan to address changes and issues identified during plan implementation or security control assessments? |  |  |  |
| Does the Agency maintain the information security plan in a secured environment to prevent its unauthorized disclosure and modification? |  |  |  |
| Develop a process to request Information Security Resources | Does the Agency consider resources (i.e., investments and human capital) needed to implement and maintain the information security plan? |  |  |  |
| Develop a Plan of Action and Milestones process | Has your Agency implemented a process for ensuring that plans of action and milestones for the security program and associated information systems are developed and maintained? |  |  |  |
| Does the Agency review plans of action and milestones for consistency with the Agency’s risk management strategy and priorities for risk response actions? |  |  |  |
| Information Security Measures of Performance | Has the Agency developed information security measures of performance based on the South Carolina Division of Information Security (SC DIS) and SC Enterprise Privacy Officer (EPO) guidance? |  |  |  |
| If so, does the Agency monitor and report (to executive management) the results of information security measures of performance? |  |  |  |
| Assigning Information Security Authority | Does the Agency’s chief executive (i.e., Agency Director, CISO) ensure that the Agency’s senior officials are given authority to secure the operations (e.g., technology) and assets (e.g., IT / network assets) under their control? |  |  |  |
| Appointing an Information Security Liaison personnel | Has your Agency appointed an information security liaison (i.e., information security officer or higher designation) with the mission and resources to coordinate, develop, implement, and maintain an information security plan? |  |  |  |
| Establish an Information Security Workforce  | Has the Agency established an information security workforce to satisfy the Agency’s information security requirements? |  |  |  |
| If so, has the Agency established a professional development program for the information security personnel? (i.e., certifications, seminars, training, etc. for the advancement of skills or expertise related to information security) |  |  |  |
| Establish a process to provide Role-Based Security Training to personnel assigned with security roles | Does the Agency provide role-based security training to personnel with assigned security roles and responsibilities (e.g., network engineer, application developer, etc.)? |  |  |  |
| Establish a process for the development of information security procedures | Does the Agency identify State and Agency specific information security objectives adopting a risk-based approach? |  |  |  |
| Does the Agency develop information security procedures which align with the identified security objectives? |  |  |  |
| Has the Agency allocated the appropriate subject matter experts (e.g., appointment of a HIPAA Privacy Officer) to the development of State and Agency-specific information security procedures? |  |  |  |
| Has the Agency approached independent external (third party) specialist to assist in the development of information security policies in cases where it is established that the required expertise do not exist within the Agency or within any other state government Agency? |  |  |  |
| Does the Agency work in collaboration with other states or Federal government agencies and external special interest groups on occasions where procedures directly or indirectly affect interfacing activities? |  |  |  |
| Do information security procedures developed by the Agency contain the following information, as required:* Revision history;
* Introduction;
* Preface;
* Ownership, roles , and responsibilities;
* Purpose;
* Policy statements;
* Policy supplements;
* Guidance; and
* Definitions?
 |  |  |  |
| Has the Agency identified and documented exceptions for scenarios that cannot be effectively addressed within the constraints of the agency’s security procedures? |  |  |  |
| Does the Agency evaluate exceptions consistently in the context of potential risk to the Agency as a whole? |  |  |  |
| Does the Agency only approve exceptions that have adequate compensation controls and cannot create significant risks? |  |  |  |
| Does the Agency reviewed draft information security procedures with applicable stakeholders to ensure that the procedure is enforceable and effective? |  |  |  |
| If so, does the Agency have a process to:* Identify gaps within information security procedures that are not enforceable and effective;
* Document the gaps; and
* Assign appropriate resources to remediate the gaps?
 |  |  |  |
| Has the Agency established a communication plan to disseminate new information security procedures or modifications to existing procedures to the Agency personnel? |  |  |  |
| Does the Agency review information security procedure documents on an annual basis to ensure these are updated and are in alignment with the State’s risk posture? |  |  |  |
| Develop processes to review and approve information security procedures | Has the Agency established a Procedure Governance Committee to review and approve information security procedures? |  |  |  |
| If so, are information security exceptions approved by the Procedure Governance Committee? |  |  |  |
| Does the Agency maintain a procedure approval history (revision history) document?  |  |  |  |
| Establish information security procedure implementation mechanisms | Has the Agency established mechanisms to ensure that the information security procedures are available to the Agency’s personnel on a continuous basis (e.g., maintaining procedures on a central repository such as a SharePoint intranet link)? |  |  |  |
| Does the Agency require employees to review and acknowledge understanding of information security procedures (e.g., accessibility agreements) before allowing such employees access to sensitive data or information systems? |  |  |  |
| Develop information security controls deployment process | Does the Agency adopt a risk-based approach to prioritize the deployment of information security controls? |  |  |  |
| Has the Agency allocated the appropriate subject matter experts to the deployment of State and Agency-specific information security controls? |  |  |  |
| Does the Agency have a process to approach an independent external (third party) specialist to assist in the deployment of information security controls in cases where it is established that the required expertise do not exist within the Agency or within any other state government Agency?(e.g., To conduct a vulnerability assessment, the Agency could employ the services of a third party which has a proven past record of conducting such assessments.) |  |  |  |
| Are information security controls which cannot be deployed due to the Agency’s resource or other constraints reported to the office of the State Chief Information Security Officer? |  |  |  |
| Does the Agency review each information security control with applicable stakeholders to ensure that the procedure is enforceable and effective? |  |  |  |
| Does the Agency have a process to:* Identify gaps within the information security controls that are not enforceable and effective;
* Document the gaps; and
* Assign appropriate resources to remediate the gaps?
 |  |  |  |
| Has the Agency established a communication plan to disseminate new information security controls or changes to existing controls to the Agency personnel? |  |  |  |
| Does the Agency reviewed controls on an annual basis to ensure these are updated and are in alignment with the State’s risk posture? |  |  |  |