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

**IT Risk Strategy 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 Information Security Measures of Performance (i.e., Metrics) and develop processes to report them | Has your agency developed a process that uses performance metrics to monitor and reports on progress in the adoption of the following:   * Statewide INFOSEC policies * Effectiveness of your Agency’s INFOSEC program, including security standards (developed by Agency), procedures, and security controls * Local and federal applicable laws and regulations (e.g., IRS 1075, HIPAA, etc.) where applicable?   (E.g., Data points for agency-developed performance metrics should be updated and reported to management regularly) |  |  |  |
| Do the performance metrics allow the Agency to identify the areas of improvement within its environment? |  |  |  |
| Develop processes to manage the metrics generated | Does the Agency ensure that the metrics collected are meaningful (e.g., specific, measureable, actionable, realistic, timely) to the Agency’s overall information system environment (e.g., network and application environment)? |  |  |  |
| Does the Agency ensure that the metrics collected yield impact and drive findings/gaps? |  |  |  |
| Do Agency metrics collected provide stakeholders with the required data points to understand and address performance gaps? |  |  |  |
| Standardizing Metrics Data Collection and Reporting | Has your Agency created standard processes to help ensure data collection, maintainance and reporting on performance metrics? |  |  |  |
| Managing External (used by third parties) Information System Services | Has your Agency developed a process to help ensure that third parties comply with:   * Statewide INFOSEC policies * Your Agency’s INFOSEC standards, procedures, and security controls * Local and federal applicable laws and regulations (e.g., IRS 1075, HIPAA, etc.) where applicable?   Process should include pre-review of controls and an ongoing compliance assessment review. |  |  |  |
| Has your Agency developed a process to conduct risk assessments on third parties, including:   * self-reporting and/or onsite reviews/audits * creation of remediation plans, and * reporting to management |  |  |  |
| Does your Agency update the third party risk assessment framework and processes in the event of:   * major changes in the scope of services provided, and * contractual changes |  |  |  |
| Establishing processes for the use of External Information Systems | Does your Agency maintain Interconnection Security Agreements (ISAs) to allow connections between internal (Agency) information systems and third party information systems? |  |  |  |
| Does your Agency document interfaces with all third parties? |  |  |  |
| If so, are the following captured in the documentation:   * Interface characteristics * Security requirements * Nature of the information being communicated |  |  |  |
| Has your Agency established the terms and conditions for interconnectivity with other entities (e.g., State agencies)?  Terms and conditions should include access controls, technical security requirements (e.g., encryption), and other controls for processing, storing or transmitting information. |  |  |  |
| Does your Agency review and update third party security agreements at least on an annual basis, or, as defined in the contracts? |  |  |  |
| Defining processes for sharing of information with Third Parties | Does your Agency share personally identifiable information (PII) with third parties, including State Agencies? |  |  |  |
| If so, is the information shared only for authorized purposes as identified in the Privacy Act, or, as indicated in the State and Federal laws? |  |  |  |
| Does your Agency use any of the following to specifically describe types of sensitive data covered and appropriate used between the Agency and third-parties?:   * Memoranda of Understanding * Memoranda of Agreement * Letters of Intent * Computer Matching Agreements * Similar agreements to the above |  |  |  |
| Does your Agency monitor, audit, and train its employees on methods of authorized sharing of sensitive data with third parties? |  |  |  |
| Does your Agency educate its employees on the consequences of unauthorized use or of sharing such data? |  |  |  |
| Evaluating new instances of sharing sensitive data | Does your Agency evaluate new / proposed instances of sharing sensitive data with third parties thereby assessing if the sharing is authorized? |  |  |  |
| Does your Agency determine if a new communication (via a public notice) needs to be generated? |  |  |  |