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

**Information Systems Acquisitions, Development and Maintenance 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 Configuration Change Management processes | Has your Agency developed a change management process to manage changes to information systems?  (e.g., changes to systems functionality, fixing bugs, and applying patches, among others) |  |  |  |
| Has this implementation of changes been controlled through the use of a change control process? |  |  |  |
| Does the change management process at your Agency require an analysis of operational impact and functionality, including impact that changes may have on other systems? |  |  |  |
| Are changes categorized and prioritized as part of the change management process? |  |  |  |
| Are changes tested and approved prior to migration to production?  (e.g., testing should typically include the user community) |  |  |  |
| If so, are the respective parties or roles responsible for approving changes defined with the Agency?  (e.g., system owner approver, development project manager, operations manager, etc.) |  |  |  |
| Does your Agency conduct a security impact analysis prior to implementation of changes? |  |  |  |
| Are post-implementation reviews performed to show changes were implemented and operating successfully? |  |  |  |
| Is an emergency change process established within the Agency? |  |  |  |
| Has the change management process, including the procedures for emergency changes, been thoroughly communicated within the Agency? |  |  |  |
| Develop Baseline Configurations for your Agency’s information systems | Does your Agency develop, review, and formally approve baseline configurations for critical information systems and infrastructure components?  (e.g., baseline configurations shall include mission critical information systems and supporting infrastructure, network devices, and key infrastructure servers and other devices) |  |  |  |
| Does your Agency develop a process to manage and document changes to baseline configurations? |  |  |  |
| Does your Agency retain older versions of baseline configurations so that a rollback is possible? |  |  |  |
| If so, are the old versions of baseline configurations stored in a secure manner? |  |  |  |
| Develop a Configuration Management Plan | Does your Agency assign separate responsibilities for developing and managing the configuration management process and to maintain daily system development activities? |  |  |  |
| Develop a System Security Plan | Has the Agency prepared a System Security Plan (SSP) for mission critical enterprise information systems? |  |  |  |
| Does your SSP provide an overview of the system’s security requirements?  (e.g., Documenting an SSP typically involves the gathering (and documentation) of the current state of the information systems. This could include details pertaining to access control, network systems, etc.) |  |  |  |
| Does your Agency update the SSP when systems are modified? |  |  |  |
| Develop a Vulnerability Management Process | Does your Agency perform a vulnerability assessment on enterprise information systems undergoing significant changes, before the systems are moved into production?  (e.g., vulnerability assessments shall be part of the change management process within the Agency) |  |  |  |
| Does your Agency perform vulnerability assessments on production enterprise information systems? |  |  |  |
| If so, are appropriate measures document, developed and implemented to address the risks associated with any identified vulnerabilities? |  |  |  |
| Does your Agency monitor and assess vulnerability notifications from vendors (e.g., notifications from Microsoft, Adobe, etc.) and additional authorized sources (e.g., third party developers (if applicable))? |  |  |  |
| Develop Information Systems Procurement Standards | Does the Agency follow the State procurement standards? |  |  |  |
| Develop a System Development and Maintenance Life Cycle | Has your Agency defined security requirements throughout the information system life cycle?  (Note: This allows lowering cost of operations, increased resource productivity, improved application security, and increased security satisfaction) |  |  |  |
| Has your Agency established a process to supervise and monitor outsourced (i.e., developed by third party) software? |  |  |  |
| Has your Agency established separate development, testing, and production environments? |  |  |  |
| Does your Agency ensure that production data is not used for testing purposes unless the data has been masked, sanitized, or declassified? |  |  |  |
| In the event that production data is used temporarily in a development environment, are appropriate security controls (including management approval, procedures to remove / delete data after completion of tests and the documentation of activities) taken by your Agency? |  |  |  |
| Has your Agency established a testing process to test controls within the information systems and controls within user development (e.g., applications developed by an Agency’s application team)? |  |  |  |
| Has your Agency established a process to select and install software patches in a timely manner? |  |  |  |
| Has your Agency established a process to collect information systems alerts, advisories, and directives on patches on a scheduled basis?  (e.g., security notifications from vendors and third party developers) |  |  |  |
| Does your Agency ensure that these security directives are in accordance within a defined schedule?  (e.g., If the Agency is to receive operating system (OS) updates, such as Microsoft’s Patch Tuesdays, does it ensure these are received as per the schedule established by the vendor?) |  |  |  |
| Has your Agency assigned a group or designated individual the responsibility of monitoring vulnerabilities and vendor releases of patches and fixes? |  |  |  |
| Does the Agency test critical operating system (OS) changes and updates in the test environment? |  |  |  |
| Does the Agency incorporate controls into information systems to check the validity of information inputs and outputs?  (e.g., during software testing, is the code tested by providing a ‘sample input’ and verifying if the output obtained is in the desired format?) |  |  |  |
| Does the Agency incorporate validation checks into information systems to detect processing errors?  (e.g., establishing a validation check for accidental deletion of data during the processing of the same) |  |  |  |
| Develop processes for Release Management | Does your Agency ensure that production-ready release packages have been deployed using the release management lifecycle, which comprises of plan, prepare, build and test, pilot, and deploy)? |  |  |  |
| Develop a Release Management Process | Does your Agency determine, as part of the release planning process:   * Resources required to deploy the release * Pass / fail criteria * Build and test plans prior to implementation * Pilot and deployment plans * Develop requirements for the release? |  |  |  |
| Develop Information Systems Documentation | Does your Agency validate the release design against the requirements, thereby identifying potential risks and issues? |  |  |  |
| Develop a mechanism to handle change requests in production | Does your Agency implement operational controls via change requests for deploying releases into production? |  |  |  |