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

**Human Resource (HR) and Security Awareness 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?** |  |  |  |
| Establish Information Security roles and responsibilities | Has the Agency defined security roles and responsibilities for the employees, contractors and third party users? |  |  |  |
| If so, has the Agency documented the security roles and responsibilities for employees, contractors and third party users according to the Agency’s information security policy? |  |  |  |
| Establish Personnel Screening procedures | Are there any State and/or Federal laws that, based on the data handled by the Agency, require that background checks are conducted on potential employees, including contractors and third parties? |  |  |  |
| If the answer to the previous question is “no”, please continue to next question.  Has the Agency implemented a process to help ensure that potential employees, contractors, and other third party personnel undergo a background check (e.g., criminal and/or credit) prior to allowing them access to sensitive data? |  |  |  |
| Establish processes for handover of Agency documents in the event of Personnel Termination and Transfer | Has the Agency documented and implemented a process and procedure for employee, contractor or third party termination and/or transfer?  The procedure that includes employee, contractor and third party responsibilities as well as responsibilities of HR, IT, Physical Security, Management, etc., with respect to the termination process |  |  |  |
| Has the Agency established a process to collect Agency documents and equipment from employees, contractors, and third party users upon termination and/or transfer? |  |  |  |
| If so, does this process require appropriate levels of approval from authorized personnel (e.g., manager)? |  |  |  |
| Establish Access Agreements for employees, contractors, and third party users | Has the Agency documented an Acceptable Use Policy that states users’ responsibilities for information security? |  |  |  |
| If so, does the Agency have its employees, contractors, and third party users agree to and sign an Acceptable Use Policy prior to receiving access to data and information systems? |  |  |  |
| Develop Role-Based Security Training based on job profiles within the Agency | Does the Agency provide security awareness training, including regular updates on the Agency’s policies and procedures to employees, contractors and third party users, according to their job function? (e.g., posters, training sessions, via email, etc.) |  |  |  |
| Has the Agency implemented a process to track participation of users on security awareness training, as well as a process to measure comprehension of key security concepts? |  |  |  |
| Does the Agency have a process to help ensure that only personnel who have successfully completed security awareness training are granted access to systems and/or sensitive data?  For instance, system administrators might require evidence of completion of training in order to enable system access. |  |  |  |
| Appointment of a Training Coordinator | Does the Agency appoint a cyber-security awareness training coordinator who is responsible to:   * Manage training content; * Establish training schedules; and * Track user training completion status |  |  |  |
| Conduct review of cyber security training content with Agency’s information security leadership? | Has the Agency implemented a process to review information security training content on an annual basis? |  |  |  |