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

**Business Continuity 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 Contingency Planning Policy and Procedures | Has your Agency documented a contingency planning policy? |  |  |  |
| If so, does the contingency planning policy address purpose, scope, roles and responsibilities and coordination among Agency departments? |  |  |  |
| Has your Agency developed procedures (e.g. business impact analysis [BIA], preventative controls, contingency strategies, testing plan, update steps, etc. to implement the contingency planning policy? |  |  |  |
| Has your Agency established a formal annual review and update process of the contingency planning policies and procedures? |  |  |  |
| Conduct a Business Impact Analysis | Has your Agency conducted a Business Impact Analysis (BIA) to identify critical processes and applications/information systems critical to the Agency? |  |  |  |
| Have the findings of the BIA, related to critical business processes, been communicated across Agency departments (e.g. business department related)? |  |  |  |
| Have the findings of the BIA, related to critical applications/information systems/ been communicated to the Agency’s IT department (e.g. IT department related)? |  |  |  |
| Based on the BIA, has your Agency determined a point in time (e.g., recovery time objective (RTO)) to determine when an interruption or disruption to the mission critical systems has an unacceptable impact on business continuity? |  |  |  |
| Have the results of the BIA driven remediation actions from potential areas of impact identified to critical business function, processes and/or application disruptions? |  |  |  |
| Has your Agency developed procedures to maintain continuity (e.g., maintaining a backup email server in the event the primary server fails) of critical business functions even if critical information systems are disrupted, breached, or, fail completely? |  |  |  |
| Designate contingency roles and responsibilities | Has your Agency designated contingency roles and responsibilities to key individuals for all business functions? |  |  |  |
| Are the above individuals aware of the responsibilities assigned for contingency planning and are they understanding of the process and procedures associated with that role? |  |  |  |
| Designate critical business partners, vendors and service providers | Has your Agency identified critical business partner, vendors, contractors and service providers? |  |  |  |
| Document, maintain and review the Agency’s Business Continuity Plan | Has your Agency documented a Business Continuity Plan (BCP)? |  |  |  |
| Based on the BCP, does your Agency utilize or address the recovery strategies to assist in addressing potential disruptions and recovery of the business functions within a defined RTO? |  |  |  |
| Besides recovery strategies, does your Agency’s BCP include the following:   * escalation and notification process * communications procedures * roles and responsibilities of designated contingency personnel * Agency critical processes * Agency critical information systems * designated alternate site * vendor management and coordination   (Note: The above list is not exhaustive and is intended for illustration purposes only. Based on an Agency’s technical environment, additional strategies might be required) |  |  |  |
| Does your Agency distribute copies of the BCP to key personnel, responsible for the recovery of the critical business functions and personnel with contingency roles, as determined by the Agency? |  |  |  |
| Has your Agency’s senior management been provided with a walk through of the BCP and have they reviewed and signed-off on the same? |  |  |  |
| Does your Agency review the BCP at scheduled intervals or, at a minimum, annually? |  |  |  |
| Does your Agency review the BCP and BIA when there are any changes internal to the Agency (organizational or operational) or the information systems the Agency utilizes? |  |  |  |
| Develop a Contingency Training Exercise | Has your Agency provided designated contingency personnel with contingency training? |  |  |  |
| Has your Agency established a process to identify individuals, assign contingency roles to them, and provide them with the necessary training? |  |  |  |
| If so, does the Agency have a method to evaluate the effectiveness of the training delivered to relevant contingency role personnel? |  |  |  |
| Has your Agency included simulated events and lessons learnt into the contingency training exercises to train the personnel with contingency roles? |  |  |  |
| Has your Agency established a frequency to conduct business contingency training (annually, at a minimum)? |  |  |  |
| Develop a plan to test the Business Continuity Plan | Does your Agency test the BCP annually in order to assess the effectiveness of the plan and the Agency’s ability to execute (e.g. readiness) the plan? |  |  |  |
| Does your Agency review the BCP test results and perform the required corrective actions? |  |  |  |
| Does your Agency document the lessons learned from the test results? |  |  |  |
| Has your Agency designated a team with responsibility to track the corrective actions and implement them in the Agency environment? |  |  |  |
| Does your Agency perform tabletop exercises or detailed simulations to test the effectiveness of the plan and identify potential weaknesses? |  |  |  |
| Conduct a Criticality Analysis | Has your Agency established processes to allow for the continuation of critical business operations while the Agency operates in an emergency mode? |  |  |  |
| Develop a Disaster Recovery Plan | Does your Agency have a Disaster Recovery Plan (DRP) for relocation of information systems that addresses the following;   * scope, * roles, * responsibilities, and * coordination among departments? |  |  |  |
| Has your Agency established RTOs for the critical information systems identified in the BIA? |  |  |  |
| Has your Agency documented restore procedures for critical information systems post an incident? |  |  |  |
| Has your Agency established and documented personnel for disaster recovery roles and responsibilities? |  |  |  |
| Has your Agency designated personnel with disaster recovery roles (e.g. crisis manager, recovery management team, IT manager, facility security manager, HR manager, customer service lead, etc.) and responsibilities? |  |  |  |
| Has your Agency documented a DRP for the recovery of critical information systems? |  |  |  |
| Has your Agency’s senior management been provided with a walk through of the DRP and have they reviewed and signed-off on the same? |  |  |  |
| Does your Agency ensure that the DRP is reviewed at scheduled intervals or, at a minimum, annually? |  |  |  |
| Does your Agency distribute copies of the DRP to key (read appointed) personnel, responsible for the recovery of the critical business functions and personnel with contingency roles, as determined by the Agency? |  |  |  |
| Has your Agency defined processes to update the DRP, when there are any changes to the Agency, information system, or the operational environment? |  |  |  |
| Establish an Alternate Site | Has your Agency designated an alternate site to recover critical business processes in disruption? |  |  |  |
| Has your Agency developed a process to relocate to an alternate site in order to resume critical business processes? |  |  |  |
| If so, has your Agency established the RTO and Recovery Point Objectives (PRO) to resume operations for business –critical functions? |  |  |  |
| If designated, does the alternate site have the required equipment and supplies to support recovery of critical business functions? |  |  |  |
| Has your Agency established contracts with third parties and suppliers for delivery of equipment/services to allow for timely recovery of critical business processes? |  |  |  |
| Does the alternate site provide security safeguards similar to the Agency’s primary site? |  |  |  |
| Has your Agency documented potential accessibility issues (e.g. network connectivity, physical access, business-critical application access, etc.) to the alternate site in the event of an area-wide disruption or disaster? |  |  |  |
| Establishing Telecommunications Services | Has your Agency established primary and alternate telecommunication service agreements with:   * Priority-of-Service provisions (aligned with RTOs) * Quality of Service (QoS) * Access   (Note: Primary telecommunications agreements are for phones utilized for everyday use. Alternate telecommunication agreements are for emergency situations) |  |  |  |
| In the event of the unavailability of primary telecommunications capabilities, has your Agency established alternate telecommunications to allow recovery of critical business processes and information systems aligned with your Agency’s RTOs? |  |  |  |
| Does your Agency require (primary and secondary) telecommunications service providers to have contingency plans? |  |  |  |
| Develop an Information System Recovery and Reconstitution Process | Has your Agency established documented procedures to restore and recover critical business after an incident? |  |  |  |
| Has your Agency implemented procedures for the recovery and reconstitution of the information system to a (previously) known state, post a disruption, compromise, or failure? |  |  |  |
| Does the Agency have the capability to restore information system components within the defined recovery time periods? |  |  |  |
| Has the Agency developed measures to protect backup and restoration hardware, firmware, and software from possible theft from the Agency location? |  |  |  |
| Establish a Data Backup and Storage Policy | Has the Agency established a Data Backup and Storage Policy? |  |  |  |
| If the Data Backup and Storage policy has been established, does it detail procedures to store data allowing recovery of information in disruption? |  |  |  |
| Does the Agency identify and apply security requirements to protect data backups based on the State of South Carolina Data Classification Schema? |  |  |  |
| Establish Data Backup Processes at the Alternate Storage Site | Has your Agency identified an alternate storage (i.e., data backup) site? |  |  |  |
| Has your Agency established what information is critical to be backed up at the alternate storage site? |  |  |  |
| Has your Agency established the required agreements with the alternate storage site to ensure the data storage and retrieval processes are not interrupted during or post an incident? |  |  |  |
| Has your Agency identified secure transfer methods when transporting backup media off-site? |  |  |  |
| Has your Agency developed a list of individuals authorized to retrieve backups from the off-site location? |  |  |  |
| Does your Agency review the security of the off-site location on an annual basis? |  |  |  |
| Information System Backup Processes | Has your Agency performed data backups of user and system-level information consistent with the Agency’s established RPOs/RTOs? |  |  |  |
| Has your Agency performed data backups of information system security documentation at a defined frequency, consistent with the Agency’s RTOs and RPOs? |  |  |  |
| Has the Agency established controls to protect the confidentiality, integrity, and availability of backup information at the storage locations?  (e.g., backed up data could be encrypted at rest, thereby protecting its confidentiality and integrity. Constant availability of backup information can be obtained by developing the required level of automation in the backup systems) |  |  |  |
| Has the Agency identified encryption methods backup data stored on the transportable media (i.e., tapes, CD Rooms, etc.)? |  |  |  |
| Does your Agency enforce a dual authorization (i.e., a two-person control) for the deletion or destruction of the Agency’s sensitive data? |  |  |  |