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

**Data Protection and Privacy 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?** |  |  |  |
| Information asset data (electronic and hard-copy) is classified into one of the following categories:* Public
* Internal Use
* Confidential
* Restricted
 | Does your Agency have a documented Data Protection and Privacy policy? |  |  |  |
| Is the policy aligned with the State of South Carolina Data Protection and Privacy Policy? |  |  |  |
| Does your Agency classify information asset data in accordance with Federal, State, regulatory and statutory guidelines? |  |  |  |
| Does your Agency use a specific tool for data classification (i.e. data inventory)?  |  |  |  |
| If you classify data, do you do so by using the State of South Carolina Data Classification Schema? |  |  |  |
| Does your Agency have personnel assigned with responsibility to classify information asset data? |  |  |  |
| Is there a periodic review of asset data classification for accuracy?  |  |  |  |
| Develop and maintain Information Labeling and Handling procedures. | Has your Agency developed procedures for Information Labeling and Handling based on data classification? |  |  |  |
| Does your Agency have an exception process whereby the information labeling and handling is not required? |  |  |  |
| Documented and implemented Acceptable Use Policy. | Does your Agency have an Acceptable Use Policy? |  |  |  |
| Does your Agency review the Acceptable Use Policy? If so, how frequently? |  |  |  |
| Are employees, contractors, and third parties made aware of the policy (e.g., signing of acceptable use policy, on-boarding training, etc.)?  |  |  |  |
| Established media sanitization processes for appropriate data disposal contained within electronic and non-electronic media. | Has your Agency developed and implemented a processes to sanitize electronic and non-electronic media prior to:* Disposal
* Reuse
* Release
 |  |  |  |
| Is the media sanitization process in compliance with the State of South Carolina Data Protection and Privacy policy? |  |  |  |
| Does your Agency track media sanitization and disposal process? |  |  |  |
| Has the Agency implemented a process to sanitize/wipe all date prior to disposal of computers, faxes, printers, flash drives, hard drives, etc.?  |  |  |  |
| Has your Agency developed documentation to provide proof of destruction / media sanitization (i.e. what, when, where, how?)  |  |  |  |
| Does your Agency maintain these records? If so, in what format (electronic or hard-copy)? |  |  |  |
| Does your Agency test media sanitization equipment and procedures annually? |  |  |  |
| ***For Federal Tax Information (FTI) receiving Agency only:*** Does your Agency sanitize electronic media containing FTI?  |  |  |  |
| ***For FTI receiving Agency only:*** Is the FTI data subject to electromagnetic erase before it is reused or released for destruction? |  |  |  |
| Does your Agency destroy hard copy media containing confidential / restricted / internal-use only information prior to their disposal? |  |  |  |
| Does your Agency assign an individual from the Agency’s Information Security department to monitor the destruction of hard copy media? |  |  |  |
| Established data protection processes for the transmission and housing of confidential or restricted information. | Do your Agency employees follow the Agency’s acceptable use policies while transmitting data? |  |  |  |
| Has your Agency developed and implemented a process and technical mechanisms to be able to access information if users lose cryptographic keys? |  |  |  |
| ***For Agencies that handle encryption keys on their own:***Has your Agency developed processes to ensure the confidentiality of private keys? |  |  |  |
| ***For Agencies that handle encryption keys on their own:***Does your Agency generate cryptographic keys using hardware-based randomization? |  |  |  |
| ***For Agencies that handle encryption keys on their own***:Does your Agency physically and logically safeguard the key-generating equipment?  |  |  |  |
| Develop cryptographic mechanisms to secure sensitive data (e.g., restricted and confidential) transfers over public / non-secure networks. | Does your Agency follow the applicable Federal or State laws and regulations pertaining to encryption of confidential data? (i.e., FIPS, AES, Triple DES, RSA, RC5, etc.?) |  |  |  |
| Has your Agency implemented encryption mechanisms to comply with the State of South Carolina Data Protection and Privacy Policy and support (at a minimum the AES 128-bit encryption standard)? |  |  |  |
| Does your Agency encrypt e-mails transmitting confidential or restricted information? |  |  |  |
| Does your Agency encrypt confidential or restricted information transmitted through the public network between the Agency, customers, vendors or partners?  |  |  |  |
| If so, does your Agency transmit this information through encrypted tunnels by using VPN, PPTP, SSL, etc.? |  |  |  |
| If you have a wireless network through which sensitive data is transferred, has this network been secured via Wi-Fi Protected Access 2 (WPA 2)?  |  |  |  |
| Has the Agency implemented Virtual Private Networks (or similar mechanisms) to secure remote network access? |  |  |  |
| Does your Agency utilize encrypted file transfer protocols (i.e. Secure File Transfer Protocol (SFTP) or Secure Copy (SCP)) to secure data transfers over the Internet? |  |  |  |
| Developed policies and procedures of use of PII and/or public web content.  | Has your Agency identified and classified what data constitutes Personal Identifiable Information (PII)? |  |  |  |
| Has your Agency conducted a Privacy Impact Assessment (PIA)? |  |  |  |
| If the PIA has been performed, has it been reviewed by your Agency’s information security personnel? |  |  |  |
| Does your Agency publish privacy policies on Agency websites used by the public? |  |  |  |
| Does your Agency update PIAs when a system change creates a new privacy risk? |  |  |  |
| Has your Agency developed confidentiality agreements defining responsibilities of the Agency’s employees and business partners/vendors to maintain privacy of electronic information? |  |  |  |