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

**Access Control 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.

pas

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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?** |  |  |  |
| Document and implement Access Control Policy and associated controls. | Does your Agency have a documented Access Control Policy? |  |  |  |
| Has your Agency documented access control procedures and associated access controls (e.g., new hire, transfer & terminated user process, obtaining privileged access, remote user access, password procedures, third-party access, etc.)? |  |  |  |
| Develop procedures in accordance with a Role Based Access Control (RBAC) model | Has your Agency developed procedures to administer privileged user access based on an RBAC model? |  |  |  |
| Develop procedures for User Account Management | Does your Agency use individual accounts? |  |  |  |
| Does your Agency use group accounts? |  |  |  |
| Does your Agency use system or application accounts? |  |  |  |
| Does your Agency use guest/anonymous accounts? |  |  |  |
| Does your Agency use temporary accounts? |  |  |  |
| For each of the different types of accounts identified above, has your Agency identified and documented specific standards, conditions, procedures and/or responsibilities to which users are held accountable once granted access to the particular type of account (if No, identify the accounts that lack documentation)? |  |  |  |
| Does your Agency authorize users and specify access rights for all information systems before provisioning and use? |  |  |  |
| Are access requests for information systems a documented procedure within the Agency? |  |  |  |
| Does your Agency maintain documentation of all user account access requests, including evidence of access approval? |  |  |  |
| Are data and/or business owners established with the Agency to approve access for each information system (as part of the access request process)? |  |  |  |
| Is the data and/or business owner identified for approving access the same as the individual responsible for owning the data within that system (e.g. the individual identified as part of the data classification exercise)? |  |  |  |
| Does the Agency authorize guest/anonymous or temporary accounts before provisioning and use? |  |  |  |
| Is the activity of the guest/anonymous or temporary account monitored? |  |  |  |
| Has the Agency established a process to notify system administrators when guest or temporary accounts are no longer needed or required? |  |  |  |
| Has the Agency established a process to notify system administrators when access rights need to be disabled or changed (e.g., termination, transfer, access changes)? |  |  |  |
| Does your Agency ensure that the minimum level of access is granted to users to perform their current job responsibilities (e.g. principals of need-to-know, least-privileged access)? |  |  |  |
| Develop Privileged User Access Management | Does your Agency grant privileged user access (e.g. access that allows the user to make mass changes such as system, network, database admins)following a formal approval process involving an information security officer / similar designated role? |  |  |  |
| Is the approval granted to individuals based on documented business need and role requirements? |  |  |  |
| Does the Agency control, monitor and report privileged accounts periodically? |  |  |  |
| Develop User Access Account Review Cycles | Does your Agency conduct reviews of user accounts periodically to ensure that:   * Access levels remain appropriate * Terminated employees do not have active accounts * Group accounts exist, if approved * No duplicate user identifiers |  |  |  |
| If the Agency conducts period reviews, is there a defined schedule? |  |  |  |
| Does your Agency review information system accounts within every 180 days? |  |  |  |
| In addition, does your Agency require information system accounts be to recertified annually? |  |  |  |
| Develop Access Enforcement Processes | Does your Agency define security requirements prior to allowing system access to contractors, vendors, business partners and other service providers? |  |  |  |
| Does your Agency implement encryption as an access control mechanism, if required by Federal, State or other laws and regulations? (e.g., encrypting data transfers, SSL) |  |  |  |
| Implement Information Flow Enforcement Processes | Has your agency developed data flows to understand source, destination, owners, data classification, etc., as a basis for access control restrictions? |  |  |  |
| Implement Separation of Duties | Does your Agency enforce separation of duties for access controls through assigned access authorizations, some of which are noted below?   * Audit function and information system access administration; * Management of critical business and information systems; * System testing and production; * Independent entity for information system security testing. |  |  |  |
| Develop the process of Least Privilege | Has your Agency implemented a process to:   1. Disable file system access not explicitly required 2. Provide minimal physical and system access to contractors 3. Require contractors’ access policy compliance 4. Grant role-based-access 5. Disable systems and removable media boot access unless authorized by the CIO   If authorized, boot access must be password protected |  |  |  |
| Processes around Unsuccessful Login Attempts | Has the Agency determined a maximum number of unsuccessful logon attempts for systems (based on classification of data hosted, processed or transferred by each information system)? |  |  |  |
| Are Agency systems capable and setup to enforce a limit on the number of unsuccessful logon attempts? |  |  |  |
| Are Agency systems capable and setup to automatically lock user accounts after the maximum number of logon attempts is reached? |  |  |  |
| Has the Agency established an account lock time period based on classification of data hosted, processed or transferred by the information system?  For example systems holding confidential or restricted data disable users indefinitely until administrator/help desk unlock user accounts. |  |  |  |
| System Use Notification | Do your Agency’s information systems display warning banners that at a minimum address the language provided by DIS in the access control policy? |  |  |  |
| Does your Agency implement warning banners, compliant with Federal, State and applicable laws associated with the type of data handled by the Agency (e.g. FTI data and IRS1075 requirements, etc.)? |  |  |  |
| Implementing a Session Lock | Are Agency systems capable and setup to end users’ sessions after thirty (30) minutes of inactivity? |  |  |  |
| Does the Agency define a maximum number of invalid logon attempts? |  |  |  |
| Does the Agency disable user access upon reaching the maximum number of invalid access? |  |  |  |
| Does the Agency keep the network and information systems locked for a predetermined amount of time or until the user regains access through the appropriate channel? |  |  |  |
| Develop processes around Remote Access | Has your Agency documented and implemented allowed methods for remote access to the network and information systems? |  |  |  |
| Does your Agency implement automated mechanism to monitor and control remote connections into the Agency network and information systems? *(For example: VPN)* |  |  |  |
| Does your Agency use Virtual Private Network (VPN) or equivalent encryption technology to establish remote access? |  |  |  |
| Do you have a policy to govern VPN access within your Agency? |  |  |  |
| Has your Agency implemented a process to managed VPN access? |  |  |  |
| Does your Agency allow users to ONLY connect using approved mechanisms (e.g., VPN tunnel) through remote access control points? |  |  |  |
| ***For Restricted data/system administrators:***  Does your Agency implement an approved two-factor authentication (2FA) technology for employees and contractors? |  |  |  |
| Does your agency have processes to allow authorized individuals to access the information systems from an external system? (e.g. alternate work site) |  |  |  |
| Develop processes around Wireless Access | For wireless access, has the Agency established:   * Usage restrictions * Configuration / connection requirements * Implementation guidance for wireless access |  |  |  |
| Does the Agency allow wireless access points to be installed independently by users? |  |  |  |
| In addition, does your Agency have the ability to identify rouge access points connecting to the wireless network? |  |  |  |
| For Agencies with wireless network:  Is the Agency wireless capable and setup to enforce user authentication? |  |  |  |
| Does the Agency have a process to explicitly approve access to wireless networks prior to enabling users with wireless access? |  |  |  |
| Develop procedures for the use of External Information Systems | If your Agency authorizes external systems, are terms and conditions for their use documented including:   * Types of applications * Categories of data processed/stored/transmitted * VPN and firewall technology use * Protection mechanisms * Maintenance and security requirements? |  |  |  |
| Develop a Boundary Protection mechanism | Has the Agency implemented controls to physically or logically segregate networks where sensitive data is stored?  For example, internal Demilitarized Zones and/or Virtual LANs can be setup to restrict network traffic between networks handling date of different classifications. |  |  |  |
| Does the Agency limit network access points to/from the Internet? (e.g., DMZ to control all Internet traffic) |  |  |  |
| Develop processes for the Identification and Authentication of users | Has the Agency established a process to enforce unique system identifiers (User IDs) assigned to each user? |  |  |  |
| Does the Agency reuse User IDs? |  |  |  |
| If so, does the Agency restrict the reuse of the unique identifier until all systems have been wiped of the previous user ID? |  |  |  |
| For agencies where group user accounts are in use:  Is each group ID identified, formally approved and business needs documented (e.g. one account shared or accessed by many employees with one shared password)? |  |  |  |
| For agencies where group user accounts are in use:  Are Agency systems capable and setup to enforce authentication via unique user IDs prior to login into a generic user ID?  For example: In Unix, a user can ‘sudo’ into the root (privileged access) account by providing their own password to the shared/group account, but the user is authenticated based on the password entered before access is granted. |  |  |  |
| Develop a multi-factor authentication process | Has the Agency chosen a multifactor authentication technique to authenticate user identity? |  |  |  |
| Develop procedures to track Unsuccessful Logon Attempts | Has the Agency implemented mechanisms to record successful and failed user log-in attempts? |  |  |  |
| Develop user provisioning for Emergency Access | Has the Agency established procedures for users to obtain access to information systems in emergency?  For example: If the Agency has a system outage/issue and requires an employee to implement a change to help fix said issue, an emergency ID could be granted which allows the user to gain excessive privileges that ordinarily are not associated with his normal, every-day ID. |  |  |  |
| Does the Agency’s emergency access procedure include the following:   * Access to live systems and data by identified and authorized personnel only * Detailed documentation of all emergency actions * Report to management |  |  |  |
| Has the Agency established a process to automatically terminate emergency accounts within twenty-four (24) hours? |  |  |  |
| Has the Agency established a process to automatically terminate temporary accounts with a fixed duration not-to-exceed three-hundred sixty-five (365) days?  For example: Temporary accounts could be granted to auditors, one-time vendors or summer interns. These temporary employees of the Agency would require access while onsite (for the day, week, month, summer, etc.), but do not need to retain access after the period of employment. |  |  |  |
| Develop password-based authentication requirements. | For network and systems within the Agency, are the following password-based requirements implemented:  Are passwords set to change every 90 days for all users? |  |  |  |
| If the Agency handles restricted data, are passwords set to change every 60 days for all users (including administrators)? |  |  |  |
| For system, database or application admins, are user account passwords changed no less than every 60 days? |  |  |  |
| For system accounts, are ID passwords changed at least every 180 days? |  |  |  |
| Is the minimum password age set to 1 day? |  |  |  |
| Is password complexity of 8 characters enabled within the Agency (e.g. upper- and lowercase letters, numbers and/or special characters)? |  |  |  |
| Does the Agency prohibit the use of dictionary names or words as passwords? |  |  |  |
| Does the Agency require a minimum number of characters to be changed when passwords are created?  *Recommended four (4) characters for restricted data* |  |  |  |
| Are passwords encrypted in storage and during transmission? |  |  |  |
| Is a password history of 6 generations enforced prior to reuse of the same password by a user? |  |  |  |
| For FTI data, does the Agency change/refresh authenticators every 90 days for standard users? |  |  |  |
| For FTI data, does the Agency change/refresh authenticators every 60 days for privileged users? |  |  |  |
| Does the Agency allow passwords to be shared among users? |  |  |  |
| If a user with privileged access is terminated or resigns, does the Agency require system passwords to be changed immediately? |  |  |  |
| Has the Agency implemented a process to change passwords due to password compromise or unauthorized use? |  |  |  |
| Develop Access Agreements for employees | Does the Agency require employees to sign an acknowledgement of understanding of password requirements prior to allowing access to network and information systems? |  |  |  |
| Implement user authentication measures | Has the Agency established a process to verify the identity of a user prior to providing a new, replacement or temporary password? |  |  |  |
| Has the Agency established a process to identify and authenticate non-Agency users? |  |  |  |
| Develop passwords management procedures | Are initial passwords set to a unique value per user and changed immediately after first use? |  |  |  |
| Does the Agency provide temporary passwords to users in a secure manner? |  |  |  |
| Does the Agency have a mechanism to prevent the use of default passwords for networks and remote applications? (e.g., for instance implementing a minimum security baseline that requires changing default passwords prior to implementing systems onto production) |  |  |  |
| Does the agency obscure authentication information during the authentication process? |  |  |  |