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

**Mobile Security 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 Device Identification Processes | If your Agency allows the use of portable devices:  Has your Agency developed a process to designate portable devices to individual owners within the Agency? |  |  |  |
| Have mechanisms to enable your Agency to sanitize devices been implemented and are in use for all portable devices?  Sanitization may be required when devices are re-purposed, designated to a new owner, and lost, among other scenarios. |  |  |  |
| For mobile devices: Has your Agency implemented mechanisms on mobile devices to remotely wipe / erase all data?  Sanitization may be required when devices are re-purposed, designated to a new owner, released out of your Agency’s control, and lost, among other scenarios. |  |  |  |
| Has your Agency established usage restrictions and configuration requirements for Agency-controlled mobile devices?  Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). |  |  |  |
| Develop access control mechanisms for mobile devices | Has your Agency established connection requirements (e.g., connecting only over a secure connection) for mobile devices? |  |  |  |
| Has your Agency established implementation guidance for Agency-controlled mobile devices?  Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). |  |  |  |
| Has your Agency developed a list of approved mobile devices?  This has a direct relation with the asset management policy, which requires that all assets are tracked by State agencies |  |  |  |
| Has your Agency implemented mechanisms to only allow authorized devices to connect to the Agencies network and systems?  For instance, technical controls (firewall white/blacklists, MAC address filtering on the network, etc.) in combination with monitoring processes. |  |  |  |
| Are the Agency’s mobile devices included in the Agency’s asset inventory identifying asset owner, location and level of access to the Agency’s network/information systems? |  |  |  |
| Has your Agency implemented encryption mechanisms on mobile devices, which are commensurate with local and federal laws and regulations? |  |  |  |
| Has your Agency implemented a process to centrally manage the installation of standard operating system, application, and patches on the mobile devices? |  |  |  |
| Does your Agency have a process implemented to remove sensitive and confidential information from the mobile device prior to their disposal? |  |  |  |
| Does the Agency implement controls to test the vendor recommended patches, hot-fixes (e.g., patch a bug in the software), or service packs before such changes are approved? |  |  |  |
| Develop processes to patch mobile devices for security flaws | Has the Agency develop a process to keep system hardware, operating system and applications up-to-date? |  |  |  |
| Has the Agency implemented a process, including associated standards to only allow mobile device applications and options which are required by users’ duties?  As per this requirement, all functions and applications without a valid business reason shall be disabled on mobile-devices. For example, users should not be given administration access onto their laptops, if not required. |  |  |  |
| Establish access controls for mobile devices | Has the Agency protected (or does it require that) all mobile devices with passwords or Personal Identification Number (PIN)? |  |  |  |
| Has this process been documented and communicated to the mobile device users? |  |  |  |
| Has the Agency implemented mechanisms on mobile devices to enforce timeout / locking? |  |  |  |
| Has your Agency developed and implemented controls to protect the data stored on mobile devices, including removable media?  For instance, memory cards from mobile devices should be encrypted and/or disabled if not required by users’ duties. |  |  |  |
| Does the Agency scan mobile devices for malicious code and viruses on an ongoing basis? |  |  |  |
| Develop security scanning procedures for mobile devices | Does the Agency scan the mobile devices for malicious code and viruses before they are allowed to connect to the network? |  |  |  |
| If mobile devices are used for transitional storage (e.g., copying data between systems), is that data deleted in a secure manner from the devices immediately after completion of such a transition? |  |  |  |
| Does the Agency have a process for mobile device users to notify designated personnel within the Agency if their device(s) are lost or stolen? |  |  |  |
| In the event that a mobile device is lost or stolen, does the Agency have a process to remote wipe / erase such devices? |  |  |  |
| Does the Agency ensure that users who require access to Agency’s information/information systems through mobile devices sign access agreements (prior to granting access)? |  |  |  |
| Establish Access Agreements with employees who are assigned mobile devices | Has the Agency established a process to train employees who have been assigned mobile devices on the safekeeping of these devices, including:   * Keeping devices in their physical presence when possible,   When stored, devices should be in a secure, out-of-sigh location |  |  |  |
| Develop procedures to train employees in the safekeeping of mobile devices | For devices that are designated for disposal:   * Has the Agency implemented a process for the safely storage of mobile devices and storage media until such devices are destroyed or sanitized? |  |  |  |
| Develop portable media protection procedures | Does your Agency sanitize or destroy information system media using Agency approved tools, mechanisms and techniques? |  |  |  |
| Has the Agency established processes to securely store portable media storage devices (e.g., CDs, flash memory devices. etc.)? |  |  |  |
| Establish portable media storage security | Has the Agency established processes to securely store non-digital (e.g., paper) media? |  |  |  |
| Does the Agency require that only secure portable storage devices (e.g., encrypted flash memory devices) are used by employees to store sensitive Agency information? |  |  |  |
| Does the Agency encrypt confidentiality of information systems stored on digital media while it is being transported outside of controlled areas? |  |  |  |
| Develop secure media transportation techniques | Does the Agency sanitize removable digital and non-digital media prior to disposal, in accordance with federal and Agency standards and policies? |  |  |  |
| Develop processes for media sanitization | Does the Agency sanitize removable digital and non-digital media prior to release outside of the Agency, in accordance with federal and Agency standards and policies? |  |  |  |
| Does the Agency sanitize removable digital and non-digital media prior to release for reuse, in accordance with federal and Agency standards and policies? |  |  |  |
| If your Agency allows the use of mobile devices:  Has your Agency developed a process to designate mobile devices to individual owners within the Agency? |  |  |  |
| Develop encryption mechanisms for portable computing devices | Does the Agency employ whole disk encryption to protect the confidentiality and integrity of information stored on mobile computing devices (e.g., laptops)? |  |  |  |
| Has the Agency established a configuration management process to address flaws and vulnerabilities on portable computing devices?  This includes patches and system updates of operating systems and applications, among other software. |  |  |  |
| Establish configuration management processes for portable computing devices | Does the Agency install hot fixes for the relevant OS?  A hotfix implies that the change may have to be made quickly and outside the normal development and testing processes established in the Agency. |  |  |  |
| Has the Agency implemented tools to automatically update virus definitions on laptops and other portable computing devices? |  |  |  |
| Does the Agency implement firewall software on laptops? |  |  |  |
| Has the Agency implemented controls to prevent users from making changes to firewall configuration on laptops? |  |  |  |
| Does the Agency have mechanisms to prevent users from installing unauthorized software on portable computing devices? |  |  |  |
| Develop processes to prevent installation of unauthorized software on portable Agency devices | Does the Agency have an approval process established for employees requiring installation of software for business use? |  |  |  |
| Does the Agency utilize asset tags (e.g., bar codes, RFIDs, etc.) to track and inventory portable computing devices? |  |  |  |
| Develop processes for appropriate asset inventory of portable media and computing devices | Has the Agency implemented a process to disable Peer-to-Peer wireless connections (also called “Ad-Hoc Connections”) on all portable computing devices? |  |  |  |