MOBILE DEVICE SECURITY POLICY

**Purpose:** The purpose of this policy is to establish safeguards for the use of state-owned mobile computing and portable media storage devices serving to protect state data, networks, and applications.

**Policy:** Mobile computing devices include laptops, hand held computers, personal digital assistants (PDAs), smart phones and portable media storage devices including, but not limited to, flash memory (memory sticks), flash cards, portable hard drives, and MP3 players.

Mobile technologies are expanding in capability while declining in cost, increasing their popularity and use by varying types of mobile workers. Although these devices offer mobility conveniences and provide productivity benefits outside of the workplace, they introduce a security risk. Given their small size and portability, key security concerns include exposure of critical information, loss or theft of devices, and virus propagation. This policy will define the physical and data security measures established to mitigate the risk of exposure and/or loss of business and confidential state agency data.

Mobile devices will only be provided when business justification and agency head approval is provided. An inventory of all mobile devices must be maintained with documentation by the responsible agency on a routine basis. The theft or loss of mobile devices must be reported immediately. Mobile devices are subject to periodic policy compliance audits by the Department of Information Technology (DoIT). The use of non-standard and/or personally owned devices is prohibited without agency authorization and approved exception.

Controlled physical access is the best defense to protect data stored on mobile computing devices. Users assigned mobile devices must abide by the following physical security requirements:

1. Device must be used only by the assigned employee; devices are not to be given to or used by any other state employee or other person.
2. Device must contain only data limited to what is required and authorized.
3. When not in use, devices must be stored in a secure environment to minimize the risk of theft or unauthorized use.
4. Device must not be left unattended in insecure areas where unauthorized access is possible.
5. Care should be taken when using devices in public areas where unauthorized viewing is possible.
6. Device must be “Shut Down” when not in use. Device must not be left in hibernate, suspend or sleep mode and should only be left in password locked/screen saver mode when in a secured area.
7. Internal and external access to state network resources requires the use of a secure VPN connection or other approved access solution.

All mobile devices will be configured/maintained with the following for safeguarding data:

1. Operating systems must be maintained with most current vendor patches and updates.
2. Only approved software should be loaded. Unauthorized software, such as games and online download programs for music and video, are not permitted to be downloaded as this software can lead to the introduction of viruses, spyware and malware as well as negatively impact device performance.
3. Login passwords are required. Do not select “remember” password option.
4. Functional options not needed should be disabled such as Bluetooth.
5. Anti-virus software must be installed and maintained.
6. Laptops must be brought in monthly and connected to the state network for a minimum of one hour to update anti-virus signatures and policy files.
7. Standard system configurations must not be changed without approval.
8. Data should not be copied onto any mobile device unless authorized by the data owner. Original data must be stored on the state network; it should never be stored on a mobile device.
9. When agency-defined confidential data is authorized to be stored locally, the State standard encryption product is required to protect data.
10. For personnel remotely accessing Payment Card Industry (PCI) cardholder data, copy, move and/or storage of cardholder data onto local hard drives and/or removable electronic media is prohibited.
11. The state standard device encryption solution must be installed on all laptops and tablets.
12. The state standard Mobile Device Management (MDM) solution must be installed on all smartphones and tablets.

The theft or loss of any mobile computing device must be reported immediately to the agency head or designee and the designated IT Liaison from the Department of Information Technology (DoIT). If the agency authorized the storage of confidential data on the mobile device or the agency believes that confidential data was stored on the mobile device, the agency must take action to comply with RSA 359-C:20. Additionally, the IT Liaison must report a security incident to the IT Security Group.

All assigned mobile computing devices must be returned to the agency head or designee when no longer required or at termination of employment. Device reassignment or disposal requires the deletion of all business data and applications.

**Accountability:** All authorized users of any state and/or agency network shall adhere to this policy.

It is the responsibility of all agency heads or their designee to enforce this policy. Employees who do not comply with this policy shall be subject to disciplinary action as outlined in the Administrative Rules of the Division of Personnel.

**Description:** This policy serves to protect state business and confidential data when stored on mobile computing and storage devices.

**Reference:**
- Personally Owned Device Policy
- IT Standards Exception Policy
- Remote Access Policy
- Data Storage and Release Policy