**Sample Mobile Device Security Policy**

**POLICY STATEMENT**

The company seeks to protect its mobile devices and the data stored on such devices, from unauthorized access, use, disclosure, alteration, modification, deletion, destruction and/or removal.

Using non-company owned/controlled mobile devices to access, use, or store sensitive company-related information, including sensitive or confidential personal information, is strictly prohibited.

**PURPOSE**

This policy describes the minimum security policy for mobile devices. Mobile devices must be appropriately secured to

* Prevent sensitive or confidential data from being lost or compromised
* Reduce the risk of spreading viruses
* Mitigate other forms of abuse of the company’s computing and information infrastructure

**SCOPE**

This policy applies to users of any mobile device that connects to the company’s network / resources or is otherwise used to store or transport company-related information.

**DEFINITIONS**

1. **Mobile Devices:** These include, but are not limited to, Personal Digital Assistants (PDAs), notebook computers, Tablet PCs, iPhones, iPads, iPods, Palm Pilots, Microsoft Pocket PCs, RIM Blackberrys, MP3 players, text pagers, smart phones, compact discs, DVD discs, memory sticks, USB drives, floppy discs and other similar devices**.**

2. **User:** Anyone with authorized access to the company’s business information systems. This includes permanent and temporary employees, third-party personnel such as temporaries, contractors, or consultants, and other parties with valid company access accounts.

3. **Screen Lock:** A password-protected mechanism used to hide data on a visual display while the device continues to operate. Screen locks can be activated manually or in response to rules.

4. **Screen Timeout:** A mechanism that turns off a device display after the device has not been used for a specified time period.

5. **Personal Information:** Informationthat can be used to identify an individual and/or an individual’s financial account(s), credit history, or credit cards, as well as individual medical record and health plan information. This includes an individual’s social security number, first name (or initial) plus last name along with his/her driver's license number or state identification card number, financial account numbers, and/or credit card number.

**ENFORCEMENT**

Non-compliance with this policy and/or its resulting procedures may be cause for disciplinary action up to and including termination. Depending on the circumstances, federal or state law may permit civil or criminal litigation and/or restitution, fines, and/or penalties for action that would violate this policy.

**RESPONSIBILITY**

1. All mobile device users are responsible for following this policy.
2. Anyone observing what appears to be a breach of security, violation of this policy, violation of state or federal law, theft, damage, or any action that might place company resources at risk must immediately report the incident to an appropriate-level supervisor, manager, or security officer.
3. Managers and supervisors are responsible for ensuring that all mobile device users in their area are aware of and understand this policy and all related procedures.

**POLICY**

1. Whenever possible, all mobile devices must be password protected. Current password standards can be found in our company security policy.
2. The physical security of these devices is the responsibility of the user to whom the device has been assigned. Mobile devices shall be kept with the user whenever possible. Whenever a device is being stored, it shall be stored in a secure place, preferably out-of-sight.
3. If a mobile device is lost or stolen, promptly report the incident to your supervisor or other person pursuant to company policy. This report should include the serial number if the device has one. If your mobile device has a serial number, record it now.
4. If sensitive or confidential documents must be stored on the device, the information must be –
	1. Encrypted, and
	2. Completely and securely removed from the mobile device before it is returned, exchanged or disposed.
5. Mobile device options and applications that are not in use should be disabled.
6. Whenever possible all mobile devices should have screen locking and screen timeout functions enabled.
7. No sensitive personal information shall be stored on mobile devices unless it is encrypted.
8. Before a mobile device is connected to company IT systems, it shall be scanned for viruses. If viruses are detected, the company may delete any files on the device. If the mobile device is used for transitional storage (for example copying data between systems), the data shall be completely and securely removed from the mobile device immediately upon completion.