**Mobile Device Policy**

1. **Definitions**

[**ORGANIZATION NAME]** **Data** - All electronically stored.

* + client confidential information
  + confidential corporate, financial, and personnel information
  + non-confidential information owned by [ORGANIZATION NAME]

**Mobile Device** - Any device that is or may be used to access or store [ORGANIZATION NAME] data while the device is outside of the offices of [ORGANIZATION NAME] including devices that are not the property of [ORGANIZATION NAME] are used to access or store [ORGANIZATION NAME] data.

\_\_\_\_ **Computer -** Any Personal Computer that is the property of [ORGANIZATION NAME] a mobile device and any Notebook/laptop Computer that is the property of [ORGANIZATION NAME].

**Private Computer -** Any Personal device used to access \_\_\_\_ (PC, MAC, smartphone, tablet , etc) that is not the property of [ORGANIZATION NAME].

1. **Scope**

This policy applies to any mobile device that accesses or stores [ORGANIZATION NAME] data.

1. **Policy**

Users are prohibited from accessing or storing [ORGANIZATION NAME] Data on a mobile device except as provided below:

1. **[ORGANIZATION NAME] Computers**

[ORGANIZATION NAME] Computers may only be used to store client confidential information and confidential corporate, financial, and personnel information if the data is encrypted on the \_\_\_ computer. Only the IT Department may install, set up, or activate encryption software on a [ORGANIZATION NAME] computer.

[ORGANIZATION NAME] computers may store non-confidential \_\_\_\_ data such as slide-deck presentations, other community education materials, and blank forms.

[ORGANIZATION NAME] computers may only access confidential \_\_\_\_\_ data through RDS software, VPN software, Remote Desktop Software or an SSL protected connection to Google Apps. Users must obtain approval of the IT Manager before using VPN software or Remote Desktop Software to access \_\_\_\_\_\_ data.

1. **Private Computers**

Private computers may only access confidential \_\_\_\_\_ data through RDS software, VPN software, Remote Desktop Software or an SSL protected connection to Google Apps. Users must obtain approval of the IT Manager before using VPN software or Remote Desktop Software to access \_\_\_\_\_\_ data.

Private Computers may store non -confidential [ORGANIZATION NAME] data such as slide-deck presentations, other community education materials, and blank forms.

1. **Personal Mobile Devices**

Personal Mobile Devices such as smartphones and tablets may only store [ORGANIZATION NAME] data if they meet the following requirements:

* The IT Department must approve the mobile device
* The IT Department must have the ability to remotely wipe all the information from the device
* The device must automatically lock after 15 minutes of non-use
* The device must require a pin or password to unlock the device

In the even the device is lost or stolen, the owner must immediately notify the IT Department so that the IT Department may initiate a remote wipe of the device. It is the responsibility of the user to back up data on the personal mobile device on a regular basis.

Personal Mobile Devices may access confidential [ORGANIZATION NAME] data through RDS software, VPN software, Remote Desktop Software or an SSL protected connection to Google Apps without meeting the above requirements so long as no confidential [ORGANIZATION NAME] data is stored on the personal mobile device. Users must obtain approval of the IT Manager before using VPN software or Remote Desktop Software to access the [ORGANIZATION NAME] data.

1. **Other Mobile Devices**

All other mobile devices, including but not limited to, memory cards, flash drives, tapes, portable hard drives, Compact Discs, DVDs, and personal cloud storage, may only be used to store client confidential information and confidential corporate, financial, and personnel information if the data is encrypted on the device. Only the IT Department may install, set up, or activate encryption software on a mobile device.

Such mobile devices may store non-confidential [ORGANIZATION NAME] data such as slide-deck presentations, other community education materials, and blank forms.

1. **Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action as detailed in the personnel policy manual or the Collective Bargaining Agreement.