[redacted]

[redacted]

Mobile Device Policy

I. Definitions

[redacted] **Data** - All electronically stored

- client confidential information
- confidential corporate, financial, and personnel information
- non-confidential information owned by [redacted]

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

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

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

II. Scope

This policy applies to any mobile device that accesses or stores [redacted] Data.

III. Policy

Users are prohibited from accessing or storing [redacted] Data on a mobile device except as provided below.

IV. [redacted] Computers

[redacted] Computers may only be used to store client confidential information and confidential corporate, financial, and personnel information if the data is encrypted on the [redacted] computer. Only The IT Department may install, setup, or activate encryption software on a [redacted] computer.

[redacted] Computers may store non-confidential [redacted] Data such as slide-deck presentations, other community education materials, and blank forms.

[redacted] Computers may only access confidential [redacted] 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 [redacted] Data.

V. Private Computers

Private Computers may only access confidential [redacted] 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 [redacted] Data.

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

VI. Personal Mobile Devices

Personal Mobile Devices such as smartphones and tablets may only store [redacted] 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 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 event 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 [redacted] 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 [redacted] 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 [redacted] Data.

VII. 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, setup, or activate encryption software on a mobile device.

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

VIII. 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.