# Mobile Device Acceptable Use Policy

All mobile device access points within the corporate firewall will be centrally managed by COMPANY’s IT department and will utilize encryption and strong authentication measures. Although IT is not able to manage the public network to which mobile devices initially connect, end-users are expected to adhere to safe and secure wireless practices while utilizing this public infrastructure.

## *Eligible Users*

Employees may use privately owned mobile device equipment for business purposes. COMPANY’s IT department must approve the handheld and connection type as being secure and protected prior to connecting to the firm’s network.

## *Policy and Appropriate Use*

It is imperative that any wireless connection used to conduct COMPANY business be utilized appropriately, responsibly, and ethically. The following guidelines must be observed:

   Employees using mobile devices and services for remote wireless access will, without exception, use secure remote access procedures. This will be enforced through the use of public/private key encryption and strong passwords in accordance with COMPANY’s password policy. The device must have the password option enabled. Employees agree to never disclose their passwords to anyone.

   Prior to initial use for connecting to the COMPANY’s network, mobile device and licensed hardware, software and related services must be activated by IT.

   Users are expected to secure all handhelds and related devices used for this activity whether or not they are actually in use and/or being carried. Any non-firm computer used to facilitate mobile device access, data transfer or software setup will have antivirus software installed.

   Employees, contractors, and temporary staff with mobile device and related wireless access privileges must ensure that their computers and handheld devices are not connected to any other network while connected to COMPANY’s network via remote access.

   The mobile device based wireless access user agrees to immediately report to his/her manager and COMPANY’s IT department any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc.

   The mobile device-based wireless access user also agrees to and accepts that his or her access and/or connection to COMPANY’s networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity.

   IT reserves the right to turn off without notice any access port to the network that puts the company’s systems, data, users, and clients at risk.

   When changing/upgrading devices, the IT department must clear the old device.

   The firm retains the right to remotely wipe any mobile device that has been misplaced or stolen.