Mobile Device Policy- Delivery

Overview

BPN-RPC's intentions for publishing a Mobile Device Policy is not to impose restrictions that are contrary to an established culture of openness, trust and integrity. BPN-RPC is committed to protecting BPN-RPC's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly, as well as manage costs for devices and track down lost or stolen devices. The purpose of this policy is to outline the acceptable use of company mobile devices at BPN-RPC. These rules are in place to protect employees, contractors and BPN-PRC. Inappropriate use exposes BPN-RPC to risks including virus attacks, compromise of network systems and services, and legal issues.

Acceptable Use

BPN-PRC owned mobile devices are to be used for business purposes in serving the interests of the company, our clients, and members during the course of normal operations. Users are responsible for exercising good judgement regarding the reasonableness of personal use. Your supervisor/manager will detail further guidelines appropriate to your position. You have a responsibility to promptly report the theft or loss of any device, or the unauthorized disclosure of BPN-RPC proprietary information. As a reminder, it is against the law to use mobile devices while driving.

MDM Access

What can we see? *Device type, phone number, carrier, installed software, memory usage, passcode, serial number, policy compliance.*

What can we do? *Remotely lock your device, locate your device, remotely wipe your device, reset your passcode, distribute applications and other content, control access to certain device functions.*

In summary, there should be no expectation of privacy when using BPN-RPC owned mobile devices.

Security Policy

All devices must be secured with a passcode, and associated accounts must have a password. Passwords must not be shared with anyone. Do not write passwords down and store then anywhere near the device.

Compliance

Any exception to the above policies must be approved by your supervisor/manager in advance. Any employee found to have violated these policies may be subject to disciplinary action, up to and including termination of employment.

Sign

_____ _____

Signature Date