# Smartphone Policy

## Overview

Smartphones are an invaluable communication mechanism in today’s workplace. Along with advanced productivity features, come increased security risks associated with malware, viruses and loss/theft. Proper management and oversight of these devices minimizes the potential for security and data incidents.

## Purpose

This policy sets forth procedures and protocols that manage smartphone related risks from personal and [LEP]-owned smartphone devices.

## Scope

This policy applies to all [LEP] staff.

## Policy

### GENERAL

Personal and [LEP] smartphones may be used to access certain functions and applications on the [LEP] network. [Insert Appropriate Department] uses a multi-layered approach to protect these devices and related information assets. Although [LEP] staff take many precautions designed to manage security and loss, phone users are ultimately responsible for the disposition of these portable devices.

Smartphones function much like a desktop computer and are equipped with many of the same features. Likewise, there are similar vulnerabilities. As with any internet attached device, malware can be downloaded to a smartphone. This can cause a variety of security problems on the local phone and to any network where the phone is connected (e.g. email). [Insert Appropriate Role] takes proactive management approaches to mitigate these risks on behalf of the [LEP] and user accessing [LEP] resources.

### DEVICE MANAGEMENT

[Insert Appropriate Department] manages all smartphones and mobile devices accessing [LEP] resources with a Mobile Device Management (MDM) platform of tools. This installs software on the local phone and manages security/access to [LEP] resources. [LEP] MDM software contains (but is not limited to) the following features:

* Application scanning
* Web Filtering and blocking as appropriate to protect against malware
* Application management that allows access private/secure information
* “Bricking” or remotely wiping smartphone data in the event the device is lost or stolen
* Drive encryption technology
* Operating system policy enforcing strong password access and screen timeouts on the phone

[Insert Appropriate Department] shall implement procedures and measures to strictly limit access to sensitive information from smartphones. Staff must adhere with all applicable [LEP] polices when using their personal smartphone for work purposes.   
  
Specific concerns around use of personal phones for business use and general policy should be discussed with the [Insert Appropriate Role].

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the [LEP]. Satisfactory examples of evidence and compliance include:

* Regular archival and current MDM device and event logs
* Anecdotal communications supporting policy implementation

## Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

## Distribution

This policy is to be distributed to all [LEP] staff.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 8/30/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |