b

IT123   
Bring Your Own Device (BYOD) Policy

|  |  |
| --- | --- |
| Status | Final |
| Version | 1.03 |
| Classification | Confidential |
| Owner | Razvan Anghelidi, Directory of IT |
| Address | 1705 Tech Avenue, Unit 3, Mississauga, ON, L4W 0A2, Canada |

*Statement of Confidentiality: This document and supporting materials contain confidential and proprietary business information of Signifi Solutions Inc. These materials may be printed or photocopied for use internally and must not be shared with other parties.*

[Document Control iii](#_Toc44606011)

[Introduction 4](#_Toc44606012)

[Audience 4](#_Toc44606013)

[Scope 4](#_Toc44606014)

[Policy Statement 5](#_Toc44606015)

[Enforcement 10](#_Toc44606016)

[Revision History 10](#_Toc44606017)

All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of Signifi Solutions Inc (from now on, Signifi). The information contained in this document is proprietary to Signifi and may not be used or disclosed except as expressly authorized in writing by Signifi.

Trademarks

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Document Control

The electronic version of this document is recognized as the only valid version.

Approval History

|  |  |  |
| --- | --- | --- |
| APPROVER(S) | TITLE/DEPARTMENT | APPROVED DATE |
| Shamira Jaffer | CEO | December 23rd, 2021 |
| Shamira Jaffer | CEO | December 7th, 2020 |
| Shamira Jaffer | CEO | July 2nd, 2020 |
|  |  |  |
|  |  |  |

## Document Sensitivity Level

Confidential

Introduction

Overview

Mobile devices, such as smartphones and tablet computers, are important tools for the organization and their use is supported to achieve business goals. However, mobile devices (personal or Signifi owned) also represent a significant risk to Signifi’s information security and data protection. If the appropriate security applications and procedures are not applied, they can be a conduit for unauthorized access to the organization’s data and IT infrastructure. This can subsequently lead to costly data leakages and system infection.

Signifi developed this mobile device policy to protect our information assets in order to safeguard our customers, intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of all mobile devices when accessing the corporate network and is intended to protect the security and integrity of Signifi data and technology infrastructure. Signifi reserves the right to restrict the use of mobile devices if users do not abide by the policies and procedures outlined below.

Audience

This policy applies to all Signifi employees, part-time and temporary workers, trainees, contractors, and vendors.

Scope

All mobile devices, whether owned by Signifi or owned by employees, that have access to corporate networks, data and systems, not including corporate IT-managed laptops. This includes smartphones and tablet computers. Limited exceptions to the policy may occur where there is a business need; however, a risk assessment must be conducted by management and written approval provided in advance.

In order to connect mobile devices to the Signifi network, employees must agree to the terms and conditions set forth in this policy, and install required software onto their mobile devices.

Policy Statement

1. Acceptable Usage

* Signifi defines acceptable business use as activities that directly or indirectly support the business of Signifi
* Signifi defines acceptable personal use on Signifi time as reasonable and limited personal communication or recreation, such as reading or game playing.
* Employees are blocked from accessing certain websites during work hours or while connected to the corporate network at the discretion of Signifi. Such websites include, but are not limited to the ones specified in the “List of Websites.xlsx” document
* Mobile devices’ cameras and video capabilities are disabled while in specified sensitive areas (marked with Do Not Film sign).

Mobile devices may not be used at any time to:

* Store or transmit illicit materials
* Store or transmit proprietary information belonging to Signifi
* Harass others
* Engage in business activities not related to Signifi

The following apps are allowed: see List of Mobile Apps.xlsx

The following apps are not allowed:

* see List of Mobile Apps.xlsx
* Any app not downloaded through Apple Store or Google Play Store.

Employees may use their personal mobile device to access the following Signifi-owned resources: email, calendars, contacts, documents.

Signifi has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

1. Mobile Devices and Support

Mobile devices must use the following operating systems: Android 10 or later or Apple iOS 16 or later.

Connectivity issues are supported by IT; however, employees should contact the device manufacturer or their carrier for operating system or hardware-related issues.

Mobile devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network. This includes the installation of mobile device management (MDM) software on all mobile devices that access the Signifi network.

Signifi Inc will support the following mobile device features utilizing the MDM software:

* Configure access to corporate Exchange email accounts
* Configure access to personal email accounts
* Configure virtual private network (VPN) settings
* Configure Wi-Fi network settings
* Enable access to the corporate directory for use in composing emails

Signifi Inc will not utilize the MDM software to:

* Track an employee’s current location or previous locations unless attempting to locate a lost or stolen device (lost or stolen devices will only be traced upon approval of the device owner)
* Access an employee’s personal or corporate emails, text messages or other messages
* Access contact information or other information stored on the device (either personal or belonging to Signifi)
* Access social networking or other applications installed on the device

1. Security

* In order to prevent unauthorized access, mobile devices must be password protected using the features of the device (Google Play password for Android devices and Apple iTunes password for iPhones).
* Passwords must contain a minimum of 12 characters. Passwords will be rotated at most every 90 days and the new password may not be one of 5 previous passwords. Password must not be the same as any other credentials used within the organization.
* The mobile device must lock itself with a password or PIN if it is idle for five minutes. The PIN should have at least 6 characters.
* Screen unlock by biometrics like retina, face or fingerprint recognition is allowed
* Screen unlock by pattern is not allowed.
* After five failed login attempts, the device will auto wipe.
* Rooted (Android) or jailbroken (iOS) mobile devices are strictly forbidden from accessing the Signifi network.
* Employees are prevented from downloading, installing and using any app that does not appear on the Signifi’s list of approved apps.
* Users must not load pirated software or illegal content onto their mobile devices.
* Users must not store Signifi data of any kind in unapproved applications on the mobile device.
* Mobile devices must be kept up-to-date with manufacturer or network provided patches. As a minimum, patches should be checked for weekly and applied at least one time per month.
* Mobile devices must not be connected to a PC or a laptop which does not have up-to-date and enabled anti-malware protection and which does not conform with Signifi’s IT policies.
* Smartphones and tablets that are not on the Signifi’s list of supported devices are not allowed to connect to the Signifi network.
* Users may not use corporate workstations to backup or synchronize mobile device content such as media files unless such content is required for legitimate business purposes.
* Employees’ access to Signifi data is limited based on user profiles defined by IT and automatically enforced.
* The employee’s mobile device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of the Signifi’s data and technology infrastructure.

1. Risks/Liabilities/Disclaimers

In the event IT must remote wipe a device, all data on the mobile device will be lost, including personal data. It is the employee’s responsibility to take additional precautions, such as backing up email, contacts, photographs, media files, etc.

Signifi reserves the right to disconnect mobile devices or disable services without notification.

Lost or stolen mobile devices must be reported to the Signifi immediately. Employees are responsible for notifying their mobile carrier upon loss of a personal mobile device.

If an employee suspects that unauthorized access to Signifi data has taken place via a mobile device, they must report the incident to their manager immediately. The manager should inform IT immediately.

The employee is expected to use his or her mobile devices in an ethical manner at all times and adhere to the Signifi’s acceptable use policy as outlined above.

The employee is personally liable for all costs associated with his or her mobile device.

The employee assumes full liability for risks including, but not limited to, the partial or complete loss of Signifi and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the mobile device unusable.

Enforcement

All instances of non-compliance will be reviewed by the department director. The department director, with the assistance of the Human Resources department has the authority to impose disciplinary actions, up to and including termination of employment or contractual agreement.

Update

This policy and all supporting documentation will be reviewed and updated annually or upon material changes to Signifi business rules, technology processes, organizational goals, or information security objectives to ensure its continuing suitability, adequacy, and effectiveness.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION | DATE | SUMMARY OF CHANGE | CHANGED BY |
| 1.0 | 2020-06-18 | First version | Muhammad Nasir |
| 1.01 | 2020-06-30 | Update to Signifi standards and particulars | Razvan Anghelidi |
| 1.02 | 2020-11-30 | Annual review | Razvan Anghelidi |
| 1.03 | 2021-12-12 | Annual review | Hadeel Alzuhairi |