North Shore Technologies

Mobile Device and BYOD Policy

Version History

Ver. No.	Release Date	Description of Change	Authored / Revised By	Reviewed By	Approved By
0.1	16th Aug 2013	First Draft	Saket Madan	Dhananjay Kumar	Ajay Kr. Zalpuri
1.0	22nd Aug 2013	Initial Release	Saket Madan	Dhananjay Kumar	Ajay Kr. Zalpuri
1.2	14th Aug 2018	Update in policy for 3.1 Technical Requirements.	Saket Madan	Dhananjay Kumar	Ajay Kr. Zalpuri
1.3	12th Sep 2019	Update in policy for 3.3 User Requirements.	Saket Madan	Dhananjay Kumar	Ajay Kr. Zalpuri
2.0	31st July 2020	Add section 4 and 5.3 for acceptable use of this policy and Risks/ Liabilities/ Disclaimers. Update section 2 for scope	Rahul Raj	Tanuj/Saket	

1. Introduction

SVAM International Inc and its affiliated companies (hereinafter referred to as "SVAM") supports Mobile devices only owned by IT team, such as smartphones and tablet computers to achieve business goals. SVAM has a requirement to protect its information assets to safeguard its customers, intellectual property, and reputation.

2. Scope

- BYOD (Bring your Own Device) culture is not followed in the organization. Only Mobile devices owned by SVAM, inclusive of smartphones and tablet computers, that have access to company wireless networks, data and systems are governed by this mobile device policy. The scope of this policy does not include IT-managed laptops.
- Exemptions: Where there is a business need to be exempted from this policy.
- Applications used by employees on their own personal devices which store or access corporate data, such as cloud storage applications, are also subject to this policy.

3. Policy

This policy is intended to protect the security and integrity of organization data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

This policy provides guidelines for the safe and productive use of mobile devices (laptop computers, tablets, smartphones, etc.) by employees. It includes requirements for users and requirements for IT departments responsible for supporting and administering mobile devices.

4. Acceptable Use

- The SVAM defines acceptable business use as activities that directly or indirectly support the business of organization.
- Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the organization. Such websites

include, but are not limited to eBay, Twitter, Amazon, Naukri.com, etc. Websites are blocked as per organization firewall policy.

- Devices may not be used at any time to:
  - Store or transmit illicit materials
  - Store or transmit proprietary information belonging to another company
  - Engage in outside business activities. Etc.
- The following apps are allowed: (such as Outlook, MS Team, official purpose apps, weather Facebook, etc., will be permitted)
- The following apps are not allowed: (Such as Entertainment App, Shopping App, Employment App, Gaming App-unless business requirement, etc. Apps not downloaded through iTunes or Google Play, etc. without permission by IT team.
- Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.
- Company has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.
- Connectivity issues are supported by IT; employees should/should not contact the device manufacturer or their carrier for operating system or hardware-related issues.
- Devices must be ready by IT for proper job functioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network and use for business purpose.

5. Principle

5.1 Technical Requirements

- Devices must use the following Operating Systems: Android 5 and above or later, iOS 5.x or later.
- Devices must store all user-saved passwords in an encrypted password store.
- Only devices managed by IT will be allowed to connect directly to the internal corporate network.
- To prevent unauthorized access, devices must be password protected using the features of the device and a strong password (as per password policy) is required to access the company network.
- The device must lock itself with a password or PIN if it is idle for five minutes.

5.2 User Requirements

- IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to official wireless network for BYOD. To connect with corporate wireless network BYOD should be connected through MAC address upon approval from the manager or in case of any business requirement or for Client visit.

- If a user suspects that unauthorized access to company data has taken place via a mobile device, they must report the incident to the IT team.
- Devices must not be “jailbroken” or “rooted” or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
- Users must not load pirated software or illegal content onto their devices.
- Applications must only be installed from official platform-owner approved sources. Installation of code from untrusted sources is forbidden. If you are unsure if an application is from an approved source contact IT team
- As per business need no patches is allowed in the mobile devises instead of this IT team have separate mobile devices for each version of Android (Version 5 and above) and iOS (Version 5 and above).
- Devices must not be connected to a PC which does not have up to date and enabled anti-malware protection and which does not comply with corporate policy.
- Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify IT team.
- IT team will maintain a daily log for Mobile In -Out Time used for business purpose.
- All mobile devices shall keep by IT team in a lock drawer.

5.3 Risks/Liabilities/Disclaimers

- Users must report all lost or stolen devices (Official) to IT Team immediately.
- The employee is expected to use his or her devices (if allocated) in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures.