Contents

[1. Introduction to Bring Your Own Device (BYOD)………………………………………………………………………. 5](#_Toc77342045)

[2. Purpose…………………………………………………………………………………………………………………………………… 5](#_Toc77342046)

[3. Scope………………………………………………………………………………………………………………………………………. 5](#_Toc77342047)

[4. BYOD DEVICES………………………………………………………………………………………………………………………… 5](#_Toc77342048)

[5. PRIVACY…………………………………………………………………………………………………………………………………… 6](#_Toc77342049)

[6. Policy……………………………………………………………………………………………………………………………………….. 6](#_Toc77342050)

[**6.1 Device Specifications** 6](#_Toc77342051)

[**6.2 User Responsibility** 6](#_Toc77342052)

[**6.3 Restrictions on authorized use** 7](#_Toc77342053)

[**6.4 Lost*,* stolen, hacked or damaged equipment** 8](#_Toc77342054)

[7. USER ACKNOWLEDGMENT AND AGREEMENT………………………………………………………………………… 8](#_Toc77342055)

**DOCUMENT REVISION CONTROL**

REVISION HISTORY

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Description of Change** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

REVIEWERS

| **Name** | **Position** | **Date** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

DISTRIBUTION

| **Date** | **Distributed to** | **Version** | **Distribution Format** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

APPROVALS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Approver** | **Title/Authority** | **Approval Remarks** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Supported Devices

|  |  |  |  |
| --- | --- | --- | --- |
| **Platform** | **Device Models** | **Operating systems** | **Applications** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**LIST OF ABBREVIATIONS**

|  |  |  |
| --- | --- | --- |
| **Index** | **Abbreviation** | **Stands For** |
| I | IT | Information Technology |
| 2 | SLA | Service Level Agreement |
| 3 | IOT | Internet of things |
| 4 | IAS | International Accounting Standards |
| 5 | FDP | Finance Department |
| 6 | ITSM | Information Technology Service Management |
| 7 | NDA | Non-Disclosure Agreement |

# 1. Introduction to Bring Your Own Device (BYOD)

This document defines framework of Bring your own device (BYOD) policy. <COMPANY NAME> has a requirement to protect its information assets to safeguard its staffs, information assets, intellectual property, and data.

BYOD Policy gives a framework for securing Information Assets which support <COMPANY NAME> with respect to IT and data security.

The devices that are usually used by users:

* Mobiles
* Tablets
* Laptops
* Portable Storage Devices

# 2. Purpose

BYOD poses a risk to information assets and systems, if not properly managed.

The purpose of this policy shall be to control the usage of BYOD, based on best practices that is essential to protect <COMPANY NAME> sensitive information, in accordance with the **[<COMPANY NAME>]** guidelines.

# 3. Scope

The scope of this document applies to all users including staff, and not limited to consultants and contractors’ parties and visitors to the <COMPANY NAME>.

Exceptions: Where <COMPANY NAME>’s needs to make exception from this policy a risk assessment must be authorized by **[IT Head & Head of Information Security]**,at <COMPANY NAME>.

# 4. BYOD DEVICES

The following devices are approved for Employee BYOD use and connecting to the <COMPANY NAME> network:

* Android Smart Phones and Tablets
* Blackberry Smart Phones and Playbook
* IOS iPhones and iPad
* [List all other devices allowed]

Before any access to company’s network, devices must be presented to IT department for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools.

# 5. PRIVACY

<COMPANY NAME> will respect the privacy of your personal device and will only request access to the device by technicians to implement security controls, as outlined below, or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings (applicable only if user downloads government email/attachments/documents to their personal device).

# 6. Policy

## **6.1 Device Specifications**

1. Proper Authorization shall be provided to user for using their own devices
2. All Devices shall use the Operating Systems that are acceptable within <COMPANY NAME>.
3. All Devices must be configured with a secure password that complies with <COMPANY NAME>, Information Security, password policy.
4. Except for devices managed by IT, devices shall not be allowed to be connected directly to the internal <COMPANY NAME> network.
5. Devices shall be kept up to date with manufacturer or network provided patches. As a minimum patch should be checked for at regular intervals, as deemed fit by <COMPANY NAME>, and applied at least once a month.
6. Devices shall not be connected to a PC which does not have up-to-date and enabled anti-malware protection and which does not comply with <COMPANY NAME> policy.
7. Devices shall be encrypted in line with <Company name>’s standards.

## **6.2 User Responsibility**

1. All devices that are brought in <COMPANY NAME> shall be used shall be disclosed by the user
2. If a user suspects that unauthorized access to organization data has taken place via a mobile device, user shall report the incident in alignment with <COMPANY NAME> immediately, as per incident Management Procedure
3. User shall not “Jailbreak”. “Jailbreak” a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.
4. Devices shall not have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
5. Users shall not load pirated software or illegal content onto their devices.
6. Applications must only be installed from <COMPANY NAME> platform-owner approved sources. Installation of code from un-trusted sources is forbidden.
7. If staff are unsure of an application is from an approved source. The user shall contact <COMPANY NAME>, Information Security Team.
8. Users shall be cautious about the merging of personal and work email accounts on their devices.
9. Users shall only load data essential to their role onto their device(s).
10. Users must report all lost or stolen devices to <COMPANY NAME>, Information Security Team, or as per the <COMPANY NAME> Policy, immediately.
11. User musk take particular care to ensure that <COMPANY NAME> data have only been sent to through <COMPANY NAME> email system. If a user suspects that information or data has been sent from a personal email account, either in body or text or as an attachment, user must notify <COMPANY NAME> Information Security Team, immediately.
12. Users must not use <COMPANY NAME> workstations to backup or synchronize device content such as media files unless such content is required for purposes.

## **6.3 Restrictions on authorized use**

* + 1. Employees whose personal devices have camera, video or recording capability are restricted from using those functions anywhere in the building or on company property at any time unless authorized in advance by management.
    2. While at work, employees are expected to exercise the same discretion in using their personal devices as is expected for the use of company devices. <Company Name> policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information and ethics apply to employee use of personal devices for work-related activities.
    3. Excessive personal calls, e-mails, or text messaging during the workday, regardless of the device used, can interfere with employee productivity and be distracting to others. Employees must handle personal matters on nonwork time and ensure that friends and family members are aware of the policy. Exceptions may be made for emergency situations and as approved in advance by management. Managers reserve the right to request employees’ cellphone bills and use reports for calls and messaging made during working hours to determine if use is excessive.
    4. Nonexempt employees may not use their personal devices for work purposes outside of their normal work schedule without authorization in advance from management. This includes reviewing, sending, and responding to e-mails or text messages, responding to phone calls, or making phone calls.
    5. Employees may not use their personal devices for work purposes during periods of unpaid leave without authorization from management. [Company Name] reserves the right to deactivate the company’s application and access on the employee’s personal device during periods of unpaid leave. An employee may not store information from or related to former employment on the company’s application. Family and friends should not use personal devices that are used for company purposes.

## **6.4 Lost, stolen, hacked or damaged equipment**

* + 1. Employees are expected to protect personal devices used for work-related purposes from loss, damage, or theft. To secure sensitive company data, employees are required to have “remote-wipe” software installed on their personal devices by the IT department prior to using the devices for work purposes. This software allows the company-related data to be erased remotely in the event the device is lost or stolen. Wiping company data may affect other applications and data.
    2. <Company Name> will not be responsible for loss or damage of personal applications or data resulting from the use of company applications or the wiping of company information. Employees must immediately notify management in the event their personal device is lost, stolen or damaged. If IT is unable to repair the device, the employee will be responsible for the cost of replacement.

# 7. USER ACKNOWLEDGMENT AND AGREEMENT

I acknowledge, understand, and will comply with the above referenced security policy and rules of behavior, as applicable to my BYOD usage of <Company name> services. I understand that business use may result in increases to my personal monthly service plan costs. I further understand that reimbursement of any business-related data/voice plan usage of my personal device is not provided.

Employee Name:

BYOD Device(s):

Employee Signature: Date: