|  |
| --- |
| Logo, company name  Description automatically generated |
| Bring your Own Device Policy |
|  |
|  |

**Version 1.0**

**Document Control**

Author

|  |  |  |
| --- | --- | --- |
| Position | Name | Location |
|  |  |  |

Revision history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Issue date | Author/editor | Description/Summary of changes |
|  |  |  |  |
|  |  |  |  |

Reviewed by

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Issue date | Name | Position | Review date |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Approvals

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Issue date | Name | Position | Approval date |
|  |  |  |  |  |
|  |  |  |  |  |

Related documents

|  |  |
| --- | --- |
| Document | Location |
|  |  |

Contents

[Bring your Own Device Policy 4](#_Toc114408267)

[Purpose 4](#_Toc114408268)

[Scope 4](#_Toc114408269)

[Definitions 4](#_Toc114408270)

[Policy Statement 5](#_Toc114408271)

[Acceptable Use 5](#_Toc114408272)

[Devices and Support 6](#_Toc114408273)

[Reimbursement 6](#_Toc114408274)

[Security: 6](#_Toc114408275)

[Risks / Liabilities / Disclaimers 7](#_Toc114408276)

[Violations 7](#_Toc114408277)

[Roles and Responsibilities 8](#_Toc114408278)

[Document Owner 8](#_Toc114408279)

[Changes, Review and Update 9](#_Toc114408280)

[Enforcement / Compliance 9](#_Toc114408281)

[Exceptions/Waiver 9](#_Toc114408282)

# Bring your Own Device Policy

## Purpose

[COMPANY NAME]’s objective for publishing an BOYD policy is to determine rules to control usage of Personal devices in a corporate usage context.

## Scope

This policy applies to all [COMPANY NAME] employees, contractors and partners.

This policy applies to all employees and contractors that have been granted permission to use their personal device for corporate usage.

## Definitions

Within this Policy, the following definitions will be used:

**Confidential Information (Sensitive Information)** – Any [COMPANY NAME] information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by [COMPANY NAME] from a third party under a non-disclosure agreement.

**Information Asset –** Any [COMPANY NAME] data in any form, and the equipment used to manage, process, or store [COMPANY NAME] data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

**Partner –** Any non-employee of [COMPANY NAME] who is contractually bound to provide some form of service to [COMPANY NAME].

**Data Classification** – the process which can be defined as a tool for categorization [COMPANY NAME] data depends on its value and importance to the company.

## Policy Statement

### Acceptable Use

The company defines acceptable business use as activities that directly or indirectly support the business of [COMPANY NAME].

Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the company. Such websites include, but are not limited to...

1. Social medias
2. Videos and TV content provider
3. Music content Provider
4. Any usual illicit or illegal websites Devices’ camera and/or video capabilities are disabled while on-site as there is no access to Customer data Devices may not be used at any time to:
   1. Store or transmit illicit materials.
   2. Store or transmit proprietary information belonging to another company
   3. Harass others
   4. Engage in outside business activities Etc. The following apps are allowed (assuming rules cited above are followed):
      1. Social medias
      2. Videos and TV content provider
      3. Music content Provider
5. The following apps are not allowed:
   1. Any usual illicit or illegal websites / apps
6. [COMPANY NAME] has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

### Devices and Support

1. Smartphones including iPhone, and Android, are allowed with the proper DLP controls approved by Information Security Department.
2. Tablets including iPad, Android, Windows are allowed with the proper DLP controls approved by Information Security Department.
3. Connectivity issues are supported by IT; employees should/should not contact the device manufacturer or their carrier for operating system or hardware-related issues.
4. 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.

### Reimbursement

1. [COMPANY NAME] will not reimburse the employee for the cost of the device.
2. [COMPANY NAME] will not reimburse the employee for the following charges: roaming, plan overages, etc.

### Security:

In order to prevent unauthorized access, Mobile Device Management solution must be installed and configured on the personal devices to access the company network with the following conditions:

1. [COMPANY NAME] password policy must be enforced by the MDM solution.
2. The device must lock itself with a password or PIN if it’s idle for five minutes.
3. After five failed login attempts, the device will lock. Contact IT to regain access.
4. Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
5. Employees are automatically prevented from downloading, installing and using any app on the work profile that does not appear on the company’s list of approved apps.
6. Employees’ access to company data is limited based on user profiles defined by IT and automatically enforced.
7. The employee’s device may be remotely wiped if the device is lost, the employee terminates his or her employment,
8. IT detects a data or policy breach, a virus or similar threat to the security of the company’s data and technology infrastructure.

### Risks / Liabilities / Disclaimers

While IT will take every precaution to prevent the employee’s personal data from being lost in the event it must remote wipe a device, it is the employee’s responsibility to take additional precautions to backup his personal data.

1. [COMPANY NAME] reserves the right to disconnect devices or disable services without notification.
2. Lost or stolen devices must be reported to the company immediately. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
3. The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company’s Acceptable Use Policy
4. The employee is personally liable for all costs associated with his or her personal device.
5. The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company 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 device unusable.
6. [COMPANY NAME] reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

## Violations

[COMPANY NAME] reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. [COMPANY NAME] does not consider conduct in violation of this policy to be within an employee’s or partner’s course and scope of employment, or the direct consequence of the discharge of the employee’s or partner’s duties. Accordingly, to the extent permitted by law, [COMPANY NAME] reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Information Security Department as soon as possible.

## Roles and Responsibilities

* **Asset Owner:** Asset Owner is responsible for tracing assets throughout the lifecycle i.e. acquisition, distribution, use and disposal. Identifying the information assets; Classifying the information assets; Labeling the information assets “whenever applicable for information assets”; Reviewing information assets classification; Communicating security controls and protection requirements to the information custodians and information users.
* **Asset Custodian:** Asset Custodian is responsible for physical and logical security of asset. Protecting [COMPANY NAME] information to ensure its confidentiality, integrity and availability; Applying information security policies and best practices to the information; Determining and documenting the requirements for authorized access to the information; Providing backup and recovery of information; Detecting and responding to security violations, security breaches and vulnerabilities; Monitoring compliance with information security policies and best practices; Reporting any suspected or actual security violations, security breaches, and incidences of compromised information to the information owner.
* **Asset User:** Asset user is responsible for protecting the asset in his custody based on the type and category of the asset. Understanding the information asset classifications, abiding by the security controls defined by the information owner and applied by the information custodians; Maintaining and conserving the information asset classification and labeling established by the information owners; Contacting the information owner when information is unmarked or the classification is unknown; Using the information only for approved [COMPANY NAME] purposes; Reporting any suspected or actual security violations, security breaches, and incidences of compromised information to the information custodian or information owner.

## Document Owner

Information Technology department

## Changes, Review and Update

1. Technological advancements and changes in the business requirements will necessitate periodic revisions to policies. Therefore, this policy may be updated to reflect changes or define new or improved requirements.
2. This document may be viewed, printed by authorized personnel only.
3. A policy review should be performed at least on an annual basis to ensure that the policy is current.
4. It is the responsibility of Information Technology Department to facilitate the review of this policy on a regular basis. Personnel and Department Head from relevant departments should also participate in the annual review of this policy.
5. Deficiencies within this policy should be immediately communicated to the Information Security Department. Policy changes should require the approval of Management.
6. Change log should be kept current and should be updated as soon as any change has been made.

## Enforcement / Compliance

1. Compliance with this policy is mandatory and all [COMPANY NAME] Departments Heads should ensure continuous compliance monitoring within their department.
2. Compliance with the statements of this policy is a matter of periodic review by the Information Security Department. Any violation will result in disciplinary action in accordance with [COMPANY NAME] process.
3. Disciplinary action will be depending on the severity of the violation which will be determined by investigations. Actions such as termination or others as deemed appropriate by executive Management should be taken.

## Exceptions/Waiver

1. This policy is intended to address information security requirements. If needed, waiver requests should be formally submitted to Security Authority, including justification and benefits attributed to the waiver.
2. The policy waiver period has maximum period of three months, and should be reassessed and re-approved, if necessary, for maximum three consecutive terms. No policy should be provided waiver for more than three consecutive terms.

End of Document