**Bring Your Own Device Policy**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

# ***Table of Contents***

[**Version Control Table**](#_1t3h5sf) **2**

[**Table of Contents**](#_4d34og8) **3**

[**Purpose**](#_1fob9te) **4**

[**Scope**](#_3znysh7) **4**

[**Policy**](#_2et92p0) **4**

[**Acceptable Use**](#_dktlkwkhaylt) **4**

[**Devices and Security**](#_rohwipe0gp0b) **4**

[**Risks, Liabilities, and Disclaimers**](#_g6vv4o7kgnx5) **5**

[**Disciplinary actions**](#_ugnv67gqgu60) **5**

[**Change, Review, and Update**](#_4ktljd6arx87) **5**

[**Responsibility**](#_g72r00tn3w51) **6**

[**Reference**](#_1ksv4uv) **6**

[**Related Documents**](#_hhcf2jf33xxn) **6**

# 

# ***Purpose***

*[Company]* gives its employees the privilege of using their personal devices, including smartphones and laptops at work for their convenience. Our company reserves the right to revoke this privilege at any time.

This policy is intended to protect the security and integrity of *[Company]* data and technology infrastructure.

There are terms and conditions set forth in this policy. *[Company]* personnel must agree to them in order to have permission to connect their devices to the company network.

# ***Scope***

This policy applies to *[Company]* personnel that seeks to use personal devices to connect to the *[Company]* network.

# ***Policy***

## ***Acceptable Use***

1. The company defines acceptable business use as activities that directly or indirectly support the business of *[Company]*.
2. The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.
3. Devices’ camera and video capabilities need not be disabled while on-site.
4. Devices may not be used at any time to:
   1. Store or transmit illicit materials
   2. Harass others
5. Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc. Meaning that software used for business purposes before installing on mobile devices should be approved by *[Company]* (Slack, Skype, etc).
6. *[Company]* has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

## ***Devices and Security***

1. Smartphones and tablets based on operating systems Android or iOS are allowed.
2. Laptops based on operating systems Windows, Linux, and macOS are allowed.
3. Devices must adhere to any policy applicable to company-owned devices, such as but not limited to the Acceptable Use Policy, Encryption Policy, and Password Policy.
4. Devices may be inspected by the IT Security Team for a security review at any time.
5. Devices with access to corporate resources should not be left anywhere in public places without overseeing
6. If needed to work in a public place - the device should be locked when you do not use it,
7. If you lose your device or it was stolen - you have to inform the Police and IT Security Team immediately.

## ***Risks, Liabilities, and Disclaimers***

1. 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, such as backing up personal data such as email, contacts, etc.
2. The company reserves the right to disconnect devices or disable services without notification.
3. Lost or stolen devices must be reported to the company immediately.
4. 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 as outlined above.
5. The employee is personally liable for all costs associated with his or her device.
6. 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.
7. *[Company]* reserves the right to take appropriate disciplinary action up to and including termination for non-compliance with this policy.

# Disciplinary actions

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Management will determine how serious an employee’s offense is and take the appropriate action.

# Change, Review, and Update

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes to this policy shall be exclusively performed by the ISMS Manager and approved by the ISMS Committee.

# Responsibility

This is the responsibility of the ISMS Manager to maintain and make sure everyone is aware of this policy.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# Related Documents