BRING YOUR OWN DEVICE TO WORK POLICY

[Organization Name] recognizes the increasing trend of employees bringing personal devices to the workplace to access company data or systems. This Bring Your Own Device (BYOD) policy aims to regulate the use of personal devices in the workplace and ensure the security and integrity of the company's data. This policy outlines the requirements and guidelines for employees who use their own devices while conducting business on behalf of [Organization Name].

SCOPE

This policy applies to all employees and contractors who wish to use their personal devices to access company data or systems. The policy applies to all types of personal devices, including but not limited to smartphones, laptops, tablets, and smartwatches.

POLICY

[Organization Name] is committed to protecting its data and systems while allowing employees to work on their preferred devices. Employees may, therefore, bring their personal devices to the workplace for business purposes, subject to the following conditions:

* All employee-owned devices that will be used to access company data or systems must be registered with the IT department. This includes smartphones, laptops, tablets, and any other device that may be used for work-related tasks.
* All devices should have the latest security updates and anti-virus software installed. Employees are responsible for keeping their devices up-to-date with the latest security patches and virus definitions. Failure to do so may result in the revocation of BYOD privileges.
* Employees should use strong passwords to protect their devices and should not share their devices with others. They are responsible for ensuring that their devices are password-protected and that passwords are not shared with anyone.
* Sensitive data should not be stored on employee-owned devices unless necessary and only after appropriate security controls have been implemented, such as encryption. Employees must adhere to all company policies regarding the protection of sensitive data.
* Employees are responsible for ensuring that their devices are secured with appropriate access controls and that only authorized individuals can access company data or systems. They must also adhere to all company policies regarding the use of company data and systems.
* Employees must comply with all applicable laws and regulations regarding the use of personal devices for work-related tasks, data privacy, and human rights. No employee using their personal device for work purposes should violate any law or regulation.

**Acceptable Use**

[Organization Name] defines acceptable business use as activities that directly or indirectly support [Organization Name]'s business.

* Employees may use their personal devices to access the following [Organization Name] electronic resources: email, calendars, contacts, directory access, the internet, and [Add more as deemed necessary].
* Employees are expected to use their device in an ethical manner at all times and not use it for any inappropriate conduct, including, but not limited to, illegal, unlawful, malicious, or prohibited purposes.
* [Organization Name] has a zero-tolerance policy for texting or emailing while driving, and only hands-free talking while driving is permitted.
* Any personal device not listed above must be reviewed with the [Insert person/department e.g., ISO] for consideration as to its applicability to this policy.
* The confidentiality of proprietary information must always be maintained.
* Any activity that could potentially cause a security breach or a disruption of service must not be engaged in.

**Support**

* Connectivity support is provided by the IT department only in the capacity of configuring devices for acceptable business use for the benefit of [Organization Name] Contact your device manufacturer or carrier for operating system or hardware-related issues.
* Employees must allow the IT department to install required software and patches on their personal devices to ensure [Organization Name] maintains a secure computing environment. Such software may include, but is not limited to, [insert required software, e.g., CMS, HRIS].
* Employees may not interfere with or alter security system software updates or installations made by the IT department.

**Risk Management and Liability Disclaimer**

* [Organization Name] reserves the right to disconnect personal devices or disable services without notification.
* Employees are personally liable for all costs associated with their personal devices.
* Employees assume full liability for risks including, but not limited to, the partial or complete loss of [Organization Name] 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.
* Lost or stolen devices with confidential company information contained within them must be reported by employees to the [Insert person/department e.g., ISO] within 24 hours.
* While the IT department will take every precaution to prevent employees’ personal data from being lost while using their personal devices for work, it is the employees’ responsibility to take additional precautions, such as backing up email, contacts, etc.

[Organization Name] reserves the right to revoke an employee's BYOD privileges if the employee violates any of the conditions outlined in this policy. Furthermore, the company will not be responsible for any damage or loss to personal devices used for business purposes. It is the employee's responsibility to ensure the safety and security of their devices.

For further information on IT security and data use and storage, please refer to [Organization Name]’s Information Technology (IT) Security Policy.

## BRING YOUR OWN DEVICE (BYOD) ACKNOWLEDGEMENT AND AGREEMENT

I acknowledge that I have read and understand [Organization Name]'s Bring Your Own Device (BYOD) policy.

I agree to:

* register my personal device(s) with the IT department and ensure that they have the latest security updates and anti-virus software installed,
* use strong passwords and will not share my device with others, and
* not store sensitive data on my personal device unless necessary and only after appropriate security controls have been implemented, such as encryption.

I understand that

* I am responsible for all costs associated with my personal device(s).
* I assume full liability for risks, including the partial or complete loss of [Organization Name]'s data and personal data due to operating system crashes, errors, bugs, viruses, malware, and/or other software or hardware failure, or programming errors that render the device unusable.
* I must report lost or stolen personal devices used for work to the [Insert person/department, e.g., ISO] within 24 hours.

By signing below,

* I agree to comply with all provisions outlined in this BYOD policy while using personal devices to access company data or systems.
* I understand that any violation of this policy may result in disciplinary action and/or revocation of my BYOD privileges.

Employee Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_