**BYOD Policy**

Creating a BYOD (Bring Your Own Device) Policy is critical before allowing the employees to access their own smartphones, laptops, and tablets within the organization’s network.

**Policy Brief and Purpose**

The BYOD Policy at [CompanyX] helps the employees understand the use and management of personal devices brought to the office be it for personal or organizational work.

**Scope**

Our BYOD policy is made for all our employees, vendors, volunteers, and partners who bring their own network-capable devices to the office. Moreover, to bring the employees of the company, we are solely responsible for our family members, guests, or visitors whom we allow to bring their devices to our workplace.

This policy also addresses the devices that use our company’s network and devices that use public networks to access our company’s data. The expectations of employees are applicable irrespective of the ass location or control.

**Acceptable Use**

- Activities that directly or indirectly promote [Company X's] business are defined as acceptable business use on company time.

- Reasonable and limited personal communication or entertainment, such as reading or game playing, is defined as acceptable personal use on company time.

- During business hours/while connected to the corporate network, employees are prohibited from visiting certain websites. The company's confidentiality Websites like these include, but are not limited to [mention prohibited websites].

- While on-site, the camera and/or video capabilities of devices are not disabled.

- At no point should devices be used to:

* Keeping or transmitting illegal materials
* Store or communicate confidential information from another organization
* Harassment of others
* Participate in outside business activities

Etc.

- The following applications are permitted: (provide a thorough list of apps that will be allowed, such as weather, productivity apps, Facebook, and so on)

- The following applications are not permitted: (Apps not available on iTunes or Google Play, for example)

- Employees can access the following company-owned resources via their mobile device: (email, calendars, contacts, documents, and so on).

- Texting or emailing while driving is prohibited at [CompanyX], and only hands-free conversation while driving is authorized.

**Devices and Support**

- Mobile phones like Android, iPhones, blackberry, and Windows are allowed at the workplace. [Mention the detailed list of the smartphones including models, versions, OS, etc.]

- Android and iOS Tablets are allowed. [list of tablets including models, OS, and version.]

- IT supports connectivity issues; employees must or must not contact the device manufacturer or their carrier for OS or hardware issues.

- Before devices can access the network, they must be presented to IT for proper job provisioning and configuration of standard apps such as browsers, office productivity software, and security tools.

**Reimbursement**

- The company will/will not reimburse the employee for a percentage of the device's cost (including the company's contribution), or the company will contribute [X] amount of money toward the device's cost.

- The company will a) pay an allowance to the employee, b) cover the entire cost of the phone/data plan, c) pay a portion of the phone/data plan, and so on.

- The company will/will not pay the employee for charges such as roaming, plan overages, and so on.

**Security**

- Devices must be protected with the password using the device's features to prevent unauthorized access, and a solid password is needed to access the company network.

- Passwords must be at least six characters long and a combination of upper- and lower-case letters, numbers, and symbols, according to the company's strict password policy. Passwords will be rotated every [X] days, and the new password cannot be the same as one of the previous 15 passwords.

- If the device is left idle for [X] minutes, it must be locked automatically with a password or PIN.

- After [X] failed logins, the device will lock automatically. The user must contact IT to regain the access.

- Rooted or Jailbroken Android or iOS devices are strictly prohibited to be accessed via company’s network.

- The employees are automatically forbidden from downloading or using any application that is not in the company’s approved apps list.

- Smartphones, tablets, and laptops that are not on the list of company’s supported devices are not/are allowed to connect to the network.

- The employee’s access to the data of the company is limited according to the user’s profile that is created by the IT and enforced automatically.

- The device may be remotely wiped, a) If the device is lost, 2) the employee's employment is terminated, or IT detects a data or policy breach, a virus, or other threat to the security of the company's data and technology infrastructure.

**Risk/Liabilities/Disclaimers**

- While IT will take every precaution to protect the employee's personal data in the event that a device must be remotely wiped, it is the employee's responsibility to take extra precautions, like backing up email, contacts, and so on.

- The company has the right to disconnect devices or disable services at any time without prior notice.

- Devices that are lost or stolen must be mentioned to the company within 24 hours. Employees are responsible for immediately notifying their mobile carrier of the loss of a device.

- The employee is expected to use his or her devices ethically at all times and to follow the company's acceptable use policy, which is outlined above.

- The employee bears sole responsibility for all costs associated with his or her device.

The employee accepts full responsibility for risks such as the partial or complete loss of company and personal data as a result of an operating system crash, errors, bugs, malware, viruses, and/or other software/hardware failures, or programming errors that render the device unusable.

- For noncompliance with this policy, [CompanyX] reserves the right to take disciplinary actions, up to and including termination.

*Disclaimer: This policy template is meant to provide general guidelines and should be used as a reference. It may not take into account all relevant local, state or federal laws and is not a legal document. Neither the author nor Springworks will assume any legal liability that may arise from the use of this policy.*