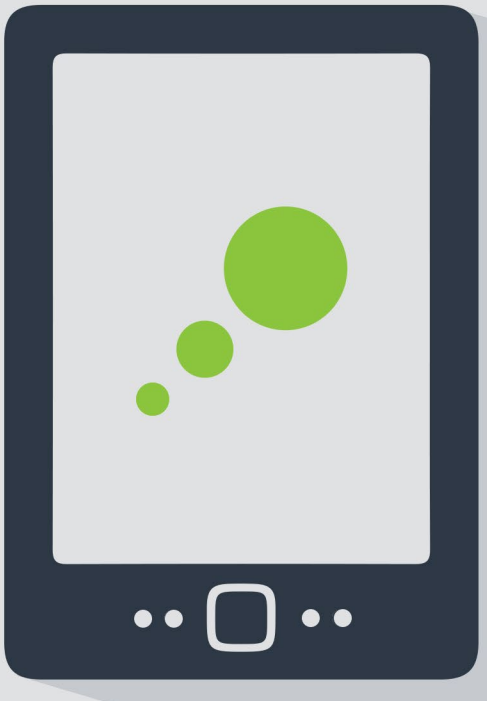

BYOD

Policy Template

cloudmore

State that this document will outline the policies, standards, and rules for personally-owned smartphones, tablets, laptops, etc. Assure that the company will respect the privacy of personal devices, and will only request access to them to implement security controls or respond to specific requests made by the employee.

Acceptable Use

- *Define acceptable business use of devices as activities that directly or indirectly support the work of "X Department."*
- *Define acceptable personal use of devices on company time as reasonable and limited personal communication or recreation, such as reading or game playing.*
- **Devices may not be used at any time to:**
  - Store or transmit illegal materials.
  - Store or transmit proprietary information.
  - Harass others.
  - *Etc.*

- **Employees may use their mobile device to access the following company-owned resources:**
  - Email
  - Calendars
  - Contacts
  - Documents
  - *Etc.*

Devices & Support

- **The following devices are supported *(list acceptable models)*:**
  - iPhone
  - iPad
  - Android
  - Windows
  - *Etc.*
- *Explain connectivity issues supported by IT; tell employees to contact the device manufacturer or carrier for operating system issues.*
- Devices should be presented to IT for proper job configuration of specific apps (such as web browsers and productivity tools) before they can access the network.

Security

- Devices must be password-protected using the features of the device, and a strong password is required to access the company network.
  - *State your company's password requirements (such as "Passwords must be six characters in length and include a combination of letters, numbers, and symbols").*
- The device must lock itself with a password or PIN if it's idle for five minutes.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Devices not on the company's list of supported devices are not allowed to access the company network.
- Employees' access to company data is limited based on user profiles defined by IT and are automatically enforced.

- **The employee's device may be remotely wiped if:**
  - The device is lost or stolen.
  - The employee terminates their employment.
  - IT detects a data or policy breach, virus, or other threat to the company's security.

Risks/Liabilities/Disclaimers

- IT will take precautions to prevent employee's personal data from being lost, but it is the employee's responsibility to take additional precautions, such as backing up emails, contacts, etc.
- The company reserves the right to disconnect or disable devices.
- Lost or stolen devices must be reported to the company within 24 hours.
- The employee is expected to use his or her devices in an ethical manner at all times.
- The employee is personally liable for all costs associated with his or her device.
- **The employee assumes full liability for risks including:**
  - Partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, or malware.
  - Programming errors that render the device unusable.

User Acknowledgement & Agreement

Have employees sign and date the document, acknowledging that they agree to comply with the above statements. Also have them list the devices they will be using.