BYOD Policy - Sample

Policy Brief and Purpose

This policy is meant to outline to rules and expectations of devices used to access organizational information. [Organization] grants its employees the privilege of purchasing and using smartphones and tablets of their choosing at work for their convenience. [Organization] reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

Scope

This document applies to any device being used to access organizational information from any organizational member whether they are an employee, board member or contractor.

Responsible use

Responsible use of a personal device includes ensuring:

- Devices are properly updated or patched to limit cybersecurity risks posed by software vulnerabilities and the device is not jailbroken (iOS) or rooted (Android).
- Basic security features such as PIN codes, passwords or biometric identification are enabled and used to prevent unauthorized access to organizational data stored or accessible on the device. The device must lock itself after being idle for a maximum of (x) minutes.
- Data encryption on the device is enabled to prevent unauthorized access to any organizational data stored on the device.
- Automatic device wiping after X failed attempts to unlock the device is enabled
- Any devices that were used to access or store and that have been lost or stolen are reported as soon as possible to the organization's IT or security team

Organizational rights

- The organizational may require you to install software or configure the device to enable remote management, policy enforcement or wiping.
- The organization reserves the right to remotely wipe your device should it have the capability to do so if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, malware 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, such as backing up email, contacts, etc.
- 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.

- 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.