SECURITY POLICY: BYOD (Bring Your Own Device)

IMPORTANT NOTE TO USER: (delete before publishing)

This is a sample policy and should not be considered a "one-size-fits-all" document. You should thoroughly read this policy and modify specific references and appropriate conditions for your organization. This document is intended to serve as a guideline and reference point for major technology considerations. *It may not reflect your specific local, state or federal laws and is not a legal document.* In addition, this document must be periodically reviewed and updated to ensure continued relevance. Under no circumstances, shall Nextrio be held liable for any language in this policy and use of this policy template constitutes your understanding of these terms and conditions.

POLICY BRIEF & PURPOSE:	Our BYOD (bring your own device) policy helps employees understand how to effectively manage personal devices (such as mobile phones, tablets, cameras, wearables, etc.) brought to the office whether for personal or business use.
SCOPE:	Our BYOD policy applies to all our employees, contractors, volunteers and partners who bring Internet/network-capable devices to our office. In addition, as employees, we are responsible for our family members, visitors and guests when we allow them to bring devices to the office. This policy addresses devices that access our company network and devices that use public networks (WiFi and cellular networks) to access company data. Employee expectations are applicable regardless of asset location or control.
REVISION HISTORY:	Version: Issue Date: Issued By:

nextrio
smart IT for business

SECURITY POLICY: BYOD (Bring Your Own Device)

This document is intended to provide guidelines for behavior and should not be considered an all-inclusive prescription for every possible situation or potential circumstance. Technology is fast-moving and ever-changing, so it is guaranteed that unanticipated scenarios will occur, even when this document is regularly updated. In all cases, our company relies on our professional employees to ask a supervisor and/or an IT manager when in doubt.

What is "BYOD"?

BYOD, which stands for "bring your own device", is a privilege that businesses can extend to enable their workforce to use the personal device of their choosing for business-related tasks. BYOD does not include company-owned equipment or devices managed and maintained by the company, although they may have similar requirements and restrictions.

Employees of our company may have the opportunity to use their personal electronic devices for work purposes when authorized in writing, in advance, by the employee and their supervisor. Personal electronic devices include, but are not limited to, personally-owned cell phones, smartphones, tablets, laptops, storage appliances, wearables, and hard/flash drives. The use of personal devices is limited to certain employees and may be limited based on compatibility of technology or suitability to the business environment.

This policy is designed to balance the convenience of permitting personally-owned devices, including mobile devices, in the workplace against risks related to the security of confidential, personal and proprietary information. It outlines permissible and impermissible uses of such devices and cautions against any expectation of privacy while these devices are connected to our company network or accessing company data and/or accounts.

Expectation of Privacy on Personal Devices

Employees choosing to use their personal devices to access company resources inherently forfeit a right to privacy on such devices. Employees agree that the company may take possession of such devices for company-related business purposes (such as a forensic investigation of a possible security breach). Furthermore, any information stored on the device, including contacts and email messages, are subject to access, retrieval and removal by the company's authorized IT staff member at any time. Notwithstanding the above waiver of privacy rights, our company will make reasonable efforts to provide advanced notice of when the device will be required and avoid access or review of personal, non-business content. The employee must realize that some incidental review of personal information is likely and there may be risk to that personal information being lost or destroyed through the course of managing the device.

The employee agrees to provide our company with access to the personal device from time to time, with or without notice, as needed in the sole discretion of our company, to perform certain security-related actions.

SECURITY POLICY: BYOD (Bring Your Own Device)

The Organization May:

- Install mobile device management software (MDM) or remote management and monitoring software (RMM) (including anti-virus/anti-malware programs where applicable) on employees' personal devices. This software will allow authorized IT staff to access, manage, monitor and remotely delete all company-related information, including calendars, e-mails and other applications. This is particularly important when a device is lost, stolen or decommissioned from service.
- Verify the device is appropriately configured to meet security standards and where necessary, reconfigure settings to meet company security requirements.
- Verify that all software/hardware updates and patches have been successfully applied.
- Scan the device for unauthorized or high-risk applications, and remove them.
- Verify that the company *Access Control* policy standards are being met.
- Monitor the device and any company resources it connects to, in its sole discretion.

The Employee Must:

- Monitor patches and updates for software/hardware as they become available and ensure they are downloaded/installed in a timely fashion.
- Use a hardened password and automatic screensaver as per the *Access Control* policy guidelines.
- Work with IT staff to ensure adequate and appropriate encryption technology is in effect on the devices and all traffic to/from the device.
- Adhere carefully to the *Digital Communications* policy and use extreme caution when opening emails and/or attachments on the device.
- Refrain from video or audio recording capability anywhere in the building or on company property at any time unless authorized in advance by their supervisor.
- Turn off or set to silent or vibrate mode any alerting device during meetings and conferences and in other locations where incoming calls and alerts may disrupt normal workflow.
- Maintain the device in its original state by not modifying its operating system or "jail breaking" the device in order to bypass built-in security features and protocols.
- Not download applications or software from unauthorized sources.
- Not intentionally or unintentionally download or transfer sensitive business data to the device.
- Report any lost or stolen device, or unauthorized access, to a supervisor as soon as discovered.
- Fully comply with our company's *Acceptable Technology Usage*, *Mobile Device Security* and *Access Control* policies.