**NSCA Sample BYOD Policy**

**Introduction:**

The purpose of this policy is to protect both the employee and the company from inappropriate, unethical or unlawful use of technology in the workplace. It is also to protect company assets and the integrity of the information residing on corporate networks. The company policies covering all intellectual property, ownership of information, licensed software, use of privileged information and other IT policies will extend to the use of employee owned mobile devices.

**What is considered BYOD?**

BYOD (bring your own device) is a common method of allowing employees to share one device for both business and personal use. It can include a smartphone, tablet, laptop or other network-connected device.

The company may also have a number of employees with COPE (company-owned, personally-enabled) devices. The BYOD policy will remain the same for COPE devices with the variation of ownership as the exception.

**Key Questions Prior to Implementation (for both internal and for client use):**

* Is there truly a business purpose for allowing employee-owned devices on the company network? Does this purpose justify the additional effort to protect the integrity of the network?
* What is your policy on licensed software and approved apps and should that extend to all devices connected to your network?
* Which web browsers and programs do you want your employees use?
* Which programs or applications will or won’t you allow to be used during work hours (i.e. You Tube, Facebook, personal email, etc.)?
* Which security tools offer the best protection for the range of devices that will be allowed to connect to the network?
* What level of support is IT expected to provide for employee-owned devices?
* How will guests and visitors be able to connect to the network? <guest WIFI rules, terms and conditions should be included here>
* Note: To make sure nothing is overlooked, get input from people across the company: HR, IT, accounting, legal – workers and executives alike.

**Company XXX Sample BYOD Policy <template>**

Institution/Company XXX grants its employees the privilege of purchasing and using employee-owned smartphones and tablets of their choosing at work for their convenience and productivity. XXX reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of XXX’s data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

XXX employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

**Acceptable Use**

* The organization defines acceptable business use as activities that directly or indirectly support the business of XXX. <edit for schools, etc.>
* The organization defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing. Personal time spent on BYOD devices will be limited to \_\_\_\_\_\_\_\_\_\_.
* Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the company. Such websites include, but are not limited to\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. <semi-annual review suggested>
* Devices’ camera and/or video capabilities are/are not disabled while on-site. Any recording must have an approved business purpose. <signs should be posted>
* Devices may not be used at any time to:
  + Store or transmit illicit materials
  + Store or transmit proprietary information belonging to another company
  + Harass, defame, or take inappropriate photos of others
  + Engage in outside business activities
  + \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, etc.
* The following apps are allowed: (include a detailed list of apps, such as weather, productivity apps, Facebook, etc., which will be permitted)
* The following apps are not allowed: (apps not downloaded through approved vendors, iTunes or Google Play, apps that have inappropriate content or images).
* Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, video conferencing, collaboration tools, projection and display systems, etc.
* XXX has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

**Devices and Support**

* Smartphones including iPhone, Android, Blackberry and Windows phones are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
* Tablets including iPad and Android are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
* Connectivity issues are supported by IT; employees should/should not contact the device manufacturer or their carrier for operating system or hardware-related issues.
* Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.
* IT is available for business-related support only.

**Security**

* Every BYOD device shall be registered and the serial number logged by IT. When updating devices, the employee shall bring in the old device along with the replacement for documentation and evaluation of information contained in memory.
* In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network.
* The company’s password policy is (example: at least six characters and a combination of upper- and lower-case letters, numbers and symbols).
* The device must lock itself with a password or PIN if it’s idle for five minutes.
* Employees are automatically prevented from downloading, installing and using any app that does not appear on the company’s list of approved apps.
* Smartphones and tablets that are not on the company’s list of supported devices are/are not allowed to connect to the network.
* Smartphones and tablets belonging to employees that are for personal use only are/are not allowed to connect to the network.
* Employees’ access to company data is limited based on user profiles defined by IT and automatically enforced.
* The employee’s device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment and has not voluntarily had the device inspected, 3) IT detects a data or policy breach, a virus 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 company reserves the right to disconnect devices or disable services without notification.
* Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their service provider immediately upon loss of a device.
* 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 is personally liable for all costs associated with his or her device.
* 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](http://www.itmanagerdaily.com/mobile-malware-grew-three-fold-last-year/), and/or other software or hardware failures, or programming errors that render the device unusable.
* XXX reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

**Optional reimbursement statements**

* The organization <will/will not> reimburse the employee for a percentage of the cost of the device (include the amount of the contribution), or the organization will contribute X amount of money toward the cost of the device.
* The organization will a) pay the employee an allowance, b) cover the cost of the entire phone/data plan, c) pay half of the phone/data plan, etc.
* The organization will/will not reimburse the employee for the following charges: roaming, plan overages, etc.
* The employee is responsible for selecting their own data plan and any unforeseen costs due to roaming charges.

**Notes:**

All users must sign, acknowledging that they have read and understand the policy.

Be sure to have legal counsel review this before implementation.

Policy can vary depending on job description and access to information as outlined in duties and responsibilities.