**Introduction: What is a Bring Your Own Device Policy?**

A Bring Your Own Device Policy (BYOD) refers to the policy of permitting employees to bring personally owned devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications.

Mission-driven organizations rely on Tech Networks of Boston to provide IT security assessments, phishing testing, security awareness training, and other managed services.

Below is a sample BYOD policy template that you can adapt to suit your organization’s needs (include additional details where it makes sense).  You may need to edit the policy to apply to different user groups with varying job requirements.

**Let us help!**

To use this template, replace your company name in the

<INSERT NAME HERE> brackets, and make a note to include

additional company policy information where needed. Be sure to

include an area for employee signature and acceptance.

**Personal Business Device (BYOD) Policy**

|  |  |
| --- | --- |
| **Policy Owner**  | <Manager of IT/Director of IT/Person responsible for IT>  |
| **Policy Objective**  | To ensure compliance and minimize risk derived from use of personal business devices.  |

Policy Statement

Personal business devices are useful for personnel who wish to perform organizational business while retaining use of a personally owned device (i.e., an Android tablet device, iPhone, iPad, or personally-owned laptop). Connection of a personal business device to <INSERT NAME HERE> systems creates a relationship between that device and <INSERT NAME HERE>, and subject certain aspects of the device’s use to Information Systems and Technology Policies and Procedures.

All personal business devices must be approved by IT in writing or email prior to connection to <INSERT NAME HERE> systems. Personal business devices must comply with the personal business device security policy at all times.

Personnel with a personal business device are on notice that IT is authorized to issue remote instructions to the device without notice, including but not limited to, a command to erase all contents.

Personnel are required to comply with requests from <INSERT NAME HERE> to monitor or review activity on personal business devices to ensure compliance with the Information Systems and Technology Policies and Procedures. After such a request is made, personnel agree to keep the device (e.g., personnel will not attempt to remove data or wipe the device) in its current state until the request has been completed.

In general, <INSERT NAME HERE> network data should not be stored on a personal business device; however, this may be authorized in certain cases. Personnel with a personal business device are required to remove all network data at the request of <INSERT NAME HERE>, or at the cessation of their relationship with <INSERT NAME HERE>. Personnel who wish to discontinue use of a personal data device may do so by wiping all data from the device per manufacturer instructions, and notifying IT in writing or email that they have done so.

Personnel with a personal business device must exercise constant caution, ensuring that the device is protected by use of a password and encryption, and that the use of the device is limited only to the person affiliated with <INSERT NAME HERE>.

**Personal Business Device Security Requirements**

Personal business devices are required to enforce the following security policies to ensure that they properly safeguard the relationship to <INSERT NAME HERE> systems and network data. The general set of policies is listed below, and will vary depending on the type and capabilities of the device.

1. Update of policy information every 180 minutes
2. Password requirement
3. Minimum password length of four (4) characters, pattern and/or biometric
4. Lockout/device deletion after ten (10) consecutive incorrect password attempts
5. Maximum time of five (5) minutes of inactivity until a password is required
6. Password expiration every ninety (90) days

All tenets of the Acceptable Use Policy apply for all personal business devices. Devices will be subject to additional policy requirements if they are expressly authorized to store information covered under <Insert any compliance requirements here, such as HIPAA, FISMA, etc.>

<INSERT NAME HERE> reserves the right to limit connection of personal business devices by use of a mobile device management (MDM) platform.

Personal business devices will only access <INSERT NAME HERE> systems and network data via an approved connection method. At no time, will a direct connection from a personal business device to systems and network data be permitted.

Current authorized connection methods include:

1. <Insert applicable connection methods here, such as ActiveSync, VPN, Remote Desktop, etc.>

Personal business devices are required to comply with the following software requirements, where applicable:

1. Be fully patched via the personal business device’s automatic update software.
2. Not be "jailbroken" or "rooted", unless expressly authorized
3. Have an up-to-date, active and functioning anti-virus program, or equivalent
4. Anti-virus must check for virus definitions weekly
5. Have an up-to-date, active and functioning anti-malware program
6. Anti-malware must check for malware definitions weekly
7. Have a personal software firewall installed and enabled, where applicable
8. Have the most recent release of its primary web browser (Internet Explorer, Safari, Firefox, Chrome, etc.)
9. Have the most recent release of Java, with automatic updates enabled

**Physical Device Care**

<INSERT NAME HERE> is not responsible for impaired operation, damage, loss, or theft of a personal business device. Personnel should consult the manufacturer for information regarding the proper care of personal business devices.

**Reimbursement**

<INSERT NAME HERE> will not reimburse the cost of a personal business device, software or license costs, or for any related expense and/or maintenance.

**User Acknowledgment and Agreement**

I acknowledge, understand and will comply with the above referenced security policy and rules of behavior, as applicable to my BYOD usage of services. <insert any language regarding reimbursement or usage here>

Employee Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

BYOD Device(s): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_