The power to do more

If your employees use their mobile devices for work purposes, a “bring your own device” policy can offer valuable protection. Use this checklist to help create a policy that’s tailored to your company’s needs.

Checklist: Protect Your Small Business with a BYOD Policy

Tablets and other mobile devices can be a boon to productivity. Yet without clear policies governing their use, you may be courting risk. If your employees store or access business data through their personal devices — but have no guidelines for keeping that data secure — a lost or hacked device could mean a costly breach.

Implementing a “bring your own device,” or BYOD, policy can help mitigate these risks. A sound BYOD policy balances productivity benefits and personal freedom with the security needs of the company. BYOD policies are not one size fits all, and not every business needs one. But for teams that use their devices as work tools, a policy can provide critical protection.

Use this checklist to help develop a BYOD policy that’s tailored to your business. When you finish, you will have a blueprint for using mobile devices productively and securely.

1. Lay the groundwork.

The first step to creating a sound BYOD policy is to understand how employees use their personal devices for work:

□ Confirm with your team which work functions they use their devices for (e.g., to read and send email, access files from the company network).

□ List the devices and operating systems employees use to connect to your network.

□ Know how employees connect to company resources — i.e., through web mail, Wi-Fi or a virtual private network (VPN).

□ Introduce the need for a security policy, as this will help prepare your staff for changes.

2. Choose policy elements.

Consider the points below to help you build a BYOD policy. Check off those that are important to protecting your business. Consult with your IT staff or outside provider to help you clarify your needs:

Device Security

□ Require complex passwords that include letters, numbers and symbols.

□ Have employees set their device to lock after a certain number of log-in attempts and after the device has been idle for a period of time (e.g., five minutes).

□ Instruct staff to install security updates on their devices, such as for browsers or operating systems, when they become available.

□ Require employees to notify you or a manager if their device is lost or stolen, and establish procedures for remotely wiping devices that contain sensitive data. Services such as **iCloud**, **Android Device Manager** and **Windows Intune** allow for this.

□ Consider encrypting files on devices, particularly if you need to comply with external regulations (e.g., HIPAA, Sarbanes-Oxley). Some newer devices include encryption features,[1] while older devices may require encryption software.

□ Decide how data stored on devices will be handled when employees leave the company. For example, your IT staff or outside provider might help employees transfer personal files to another device.

Acceptable use

□ Provide guidelines for apps that staff should not download. For example, you might prohibit downloads from unknown sources to help reduce the risk of malware.

□ Instruct your team to avoid clicking on suspicious links using their mobile devices, as they would on a PC.

□ Require employees to use a VPN to access the company network remotely,[2] or at the least, to avoid using public Wi-Fi networks.

Reimbursement

□ Decide if you will cover the cost or a portion of the cost of employees' phone/data plans. Also make clear under what circumstances you will reimburse for plan overages or roaming charges.

□ Determine whether you will reimburse employees a percentage or set dollar amount toward new devices.

Enforcement

□ Decide how you will enforce the policy. For example, malware infiltration caused by downloading an app from an unfamiliar source may result in a warning or loss of company contribution toward phone/data costs.

3. Draft, refine and implement your BYOD policy.

Work with key employees and your IT staff or provider to develop your policy, incorporating the elements you've checked in Parts 1 and 2. Then, take these steps before implementing your policy:

□ Share the policy with your team and answer questions.

□ Refine the policy based on questions and feedback.

□ Have employees sign the policy.

□ If needed, provide training to help employees adopt elements of the policy (e.g., using encryption software).

□ Enforce the policy according to the guidelines you have set.

□ Review the policy at least yearly to be sure it still meets your team's needs and your security requirements.

□ Update the policy as needed.

A sound BYOD policy can help your company reap the full productivity benefits of using tablets and other mobile devices. To learn more about how to get the most from tablets, read this **article** and these **examples**. To see how businesses in a range of industries use tablets to work more productively, check out this **infographic**.

Dell™ Venue Windows and Android tablets offer superior performance and a range of features to help improve collaboration and productivity.

Learn More Online
or Call **1-800-456-3355.**

[1] BitLocker Drive Encryption is available with Windows 8 Pro license.

[2] Ability to connect device to a company domain is available with Windows 8 Pro license.

The power to do more