mobile mentor

Securing Hybrid Workers with Personal Devices

THE GUIDE TO BUILDING A SUCCESSFUL BYOD PROGRAM

“We get 320,000 attacks every day, mostly by email and many of those come through BYO devices.”

J Britton Tabor, EVP Erianger Health Systems

CONTENTS

Bring Your Own Device

Embracing hybrid work with personal devices

Hybrid workers are using personal devices for work more than ever. Millions of people use their own laptop and smartphone to access company email, Teams and OneDrive.

This can be advantageous to many businesses looking to save on the cost of devices, but when companies fail to properly secure company data on personal devices it leaves a major security vulnerability.

According to the 2022 Endpoint Ecosystem study, 64% of people use a personal device for work but only 43% of those devices have BYOD securely enabled. That means roughly one quarter of the workforce has no security on their personal devices.

Does your BYOD Program look like this?

The Litmus Test

Can your employee use their personal Apple ID to download Microsoft 365 apps from the Appstore onto their personal iPhone? And then can they sign-in to their Office 365 account?

If so, your company data (OneDrive, email attachments, contact lists) is now accessible in an unmanaged app, on an unmanaged device.

Worst of all, your IT department has zero visibility of this as it is all outside the company compliance framework (personal device, public app and personal Apple ID).

Empowering Your Employees with BYOD

Understandably, many employees don't want to give control of their personal devices to their company's IT team. Employees see this as an invasion of privacy. In some industries like healthcare, BYOD is such a toxic subject that employees will change jobs if they perceive their employer is over-stepping the boundaries.

The debate around enrolling devices has been a source of intense friction between IT leaders and end-users for almost 15 years and unfortunately, that old wound is still raw. COVID, working from home, and the shift to hybrid work has poured salt on the wound.

Fortunately, there are ways to reduce the BYOD risk without managing the employee's device.

It requires three inter-linked strategies:

01 A thoughtful approach to the BYOD policy to achieve broad consensus

02 Careful selection of the appropriate technical controls with a tiered trust model

03 Messaging that explicitly addresses employee privacy together with data security

A Good BYOD Program is Empowering

When done well, BYOD can be empowering. It grants businesses the ability to secure company data on personal devices while assuring employees that their privacy is respected. A good BYOD program helps companies to attract talent and motivate employees to work longer hours. The juice is worth the squeeze.

This whitepaper outlines best practices for each of these three strategies based on our first-hand experience over the past 15 years. It is not intended to be all-encompassing and since every business is different, there is no one-size-fits-all approach.

Mobile Mentor will make BYOD a success in your company by developing your policy, designing controls and drafting messaging to ensure you land the program

Step 1:

Creating Balanced BYOD Policy Guidelines

Businesses need to consider a wide range of issues when defining policy for a modern mobile workforce, especially if some of the mobile fleet consists of BYO devices.

The **policy needs to balance** the interests of the employer (security, cost control and liability) and the concerns of the employee (privacy protection, device management and financial reimbursement).

The **most important stakeholders** for mobile policy development are Finance, IT, HR, the employees and sometimes the unions. Each group has a different set of considerations for a mobile policy.

It is easy to take a policy template from another company and adapt it to your business but there is a risk that it may take **2 years** to get everyone aligned so that the policy can be formally approved by senior leadership. To achieve the same outcome in **1 month**, we recommend a facilitated process with a series of workshops and review milestones.

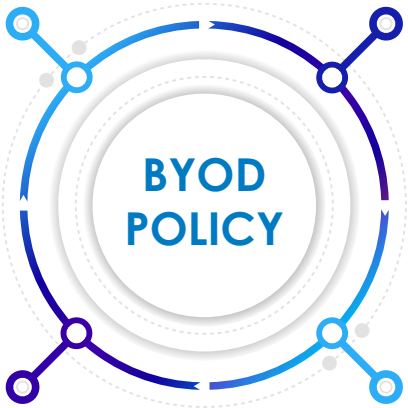
Mobile devices are very personal and in our 15 years developing mobile policies we have learned that all the stakeholders have strong opinions about BYOD and how it should be managed. Sometimes these opinions are emotionally charged so an objective facilitator can help.

Essential Considerations of BYOD Policy

When you're beginning your BYOD journey, you'll need to consult with key decision makers in different parts of your company to understand their unique needs. Each functional area will have specific considerations that will help you shape a balanced BYOD policy.

Finance Considerations

- Cost management
- Risk and liability
- Existing carrier contracts



HR Considerations

- Safe driving practices
- User profiling
- Stipend model

Security Considerations

- Microsoft 365 data
- Device security
- Groups and profiles
- Threat protection

Employee Considerations:

- Privacy protection
- Minimum OS version
- Email & Microsoft 365 access

Step 2:

Determining Your Tiered Trust Model

Not everyone in your company will have the same needs when it comes to security and privacy. This is why it is important to define the security and privacy requirements for each persona and use case.

No Trust

Unmanaged BYO Devices that access data which is public or considered low-risk

Low Trust

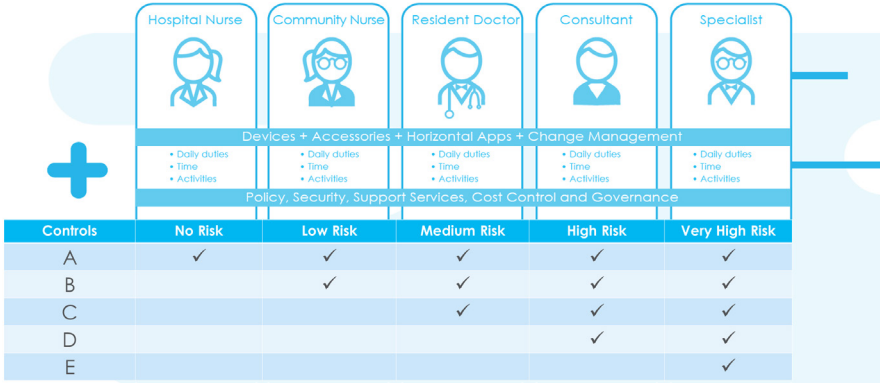
Unmanaged BYO Devices that access Microsoft 365 via OWA and Web Applications

Medium Trust

Unmanaged BYO Devices with managed Microsoft 365 Apps on the device

High Trust

Managed BYO Devices with managed apps that access Microsoft 365 and other apps



Controls	No Risk	Low Risk	Medium Risk	High Risk	Very High Risk
A	✓	✓	✓	✓	✓
B		✓	✓	✓	✓
C			✓	✓	✓
D				✓	✓
E					✓

Step 3:

Establishing the Right Method of Management

Based on the unique needs or your business, you'll want to carefully consider what method of device management suits your security and privacy needs. It is important to consider that all device operating systems have different controls in place on BYO devices.

There are four fundamental methods of device management to consider:

1. Full MDM Enrollment
2. User Enrollment
3. MAM (Mobile Application Management)
4. Unmanaged

Full MDM Enrollment

This is a method used for corporate devices. This management strategy requires employees to install a management profile on their personal mobile devices, effectively enabling businesses to manage and secure devices.

Full MDM enrollment allows IT teams to monitor device activity and fully control access to corporate resources. It also allows for the enforcement of security policies and the ability to wipe devices in the event of loss or theft.
Read our Full MDM Guide

Note – Full enrollment is not an option with BYOD android

Full MDM Enrollment

Payoffs of Full MDM:

Enhanced Security:
Full MDM enrollment enables strong security policies on employee devices, such as requiring passcodes, encryption, and automatic updates. This can reduce the risk of data breaches and protect sensitive corporate information.

Comprehensive Control:
Full MDM enrollment enables IT team to gain greater control over employee devices, including the ability to remotely wipe them in case of loss or theft. This can prevent sensitive data from falling into the wrong hands.

Compliance:
Full MDM enrollment helps businesses meet regulatory compliance requirements, such as those related to data privacy and security.

Improved productivity:
By providing secure access to corporate resources, Full MDM enrollment can help employees work more efficiently and effectively.

Considerations of Full MDM:

Privacy:
If configured incorrectly, full MDM enrollment can give your business access to personal data on an employee's device, which may raise privacy concerns.

Cost:
The price of full MDM enrollment can add up as it often requires IT support.

Complexity:
Full MDM enrollment can be complex and time-consuming, as it requires significant setup and ongoing management.

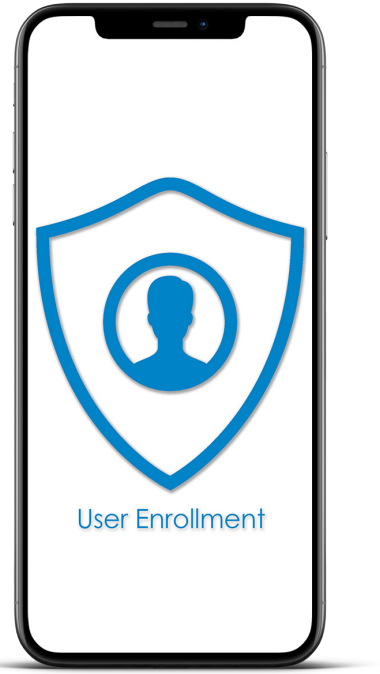
iPadOS/ iOS:
Full MDM enrollment helps businesses meet regulatory compliance requirements, such as those related to data privacy and security.

Android:
Full MDM enrollment for BYOD devices is only applicable to devices with Android Enterprise. However, from here you can create work and personal profiles that enable access to company resources for users to run in split mode.

User Enrollment

User enrollment in a BYOD program requires users to install a management app on their personal devices which enables your IT team to manage and secure those devices.

This approach involves minimal control over the device itself, however, a similar support effort to Full MDM enrollment is required for User Enrollment success.



User Enrollment

Payoffs of User Enrollment:

Enhanced Security:
User enrollment can enhance security by providing your business with greater control over the apps and data that reside on employee devices. Enable your IT team to enforce stronger security policies and prevent unauthorized access to sensitive information.

Reduced Costs:
User enrollment can be less expensive than full MDM enrollment, as it does not require as much hardware or IT support.

Simplified Management:
User enrollment can simplify device management, as it allows your business to focus on managing the apps and data that reside on the device, rather than the device itself.

Considerations of User Enrollment:

Limited Control:
Your business will have limited control over the device itself, which can limit some of your ability to enforce security policies.

Compliance Concerns:
User enrollment may not be sufficient to meet regulatory compliance requirements, as it may not provide adequate control over the device that some industries require.

MAM: Mobile Application Management

Applicable only to mobile devices (iOS/iPadOS/Android). MAM allows your IT team to manage and secure corporate apps and data on employee devices without the need for control over the entire device.

This strategy enables your business to control the apps and data your employees use for work while simultaneously respecting their privacy and freedom to use their personal devices as they choose.

MAM: Mobile Application Management

Payoffs of MAM:

Improved Productivity:
By providing secure access to corporate apps and data, full MAM only can help employees work more efficiently and effectively.

Greater Flexibility:
MAM can allow employees to use their own devices for work purposes, while still ensuring that corporate data is secure.

Data Security:
The ability to remove work data from the device is streamlined without needing control of any personal data or the BYOD device.

Easy Activation:
One of the advantages of MAM that many teams find to be a selling point is the simplicity of activation. Intune offers a range of features that simplify the application process including a wide range of policy options, app deployment options, app wrapping and SDK integration and an intuitive admin console.

Considerations of MAM:

Limited Control:
Your business will have limited control over the device itself, which can limit some of your ability to enforce security policies.

Unmanaged

An unmanaged strategy in a BYOD (Bring Your Own Device) program refers to the practice of allowing employees to use their personal devices for work purposes without any management or security controls from the organization.

This approach essentially treats the employee's device as an external entity and does not provide any form of corporate control or management over the device or the data on it.

Risks of unmanaged devices

Reduced Security:
An unmanaged strategy can increase the risk of data breaches, as your business has no control over the device or the apps and data on it. This can lead to data loss, theft, or unauthorized access.

Compliance Concerns:
Your business will have no control over the device itself, which can limit some of your ability to enforce security policies.

Limited Control:
An unmanaged strategy does not provide your business with any control over the device or the data on it, which can limit the ability to enforce security policies and protect sensitive information.

Rollout and Messaging

When rolling out your BYOD program to employees, defining your program as a sensible compromise between employee privacy and company security is a great place to start. Effective communication and messaging are crucial to ensure understanding, cooperation, and a smooth transition.

Here are some tips to make sure the communication process goes smoothly:

1. **Clearly define the program:**

   Begin by creating a clear and concise description of the BYOD program. Define what it means, the objectives, benefits, and any guidelines or policies associated with it. Make sure to address any security measures that will be implemented to protect both the company's data and the employees' personal information.

2. **Develop a communication plan:**

   Outline a comprehensive communication plan that includes multiple channels to reach all employees. This plan should include emails, presentations, intranet posts, town hall meetings, or even one-on-one sessions. Tailor the messaging to different audiences within the business, such as IT, HR, and various departments.

3. **Highlight the benefits:**

   Play up the advantages of the BYOD program for both the company and employees. This could include increased flexibility, increased productivity, cost savings, and the ability to use preferred devices. Clearly explain how the program aligns with the organization's goals and values.

Rollout and Messaging

4. **Address Privacy Concerns:**

   Address any privacy concerns upfront to build confidence in the program. Provide guidelines on how employees can protect their personal devices and ensure they understand their responsibility in safeguarding company data.

5. **Provide Training and Support:**

   Offer comprehensive training to employees on how to securely set up their devices for work purposes. Provide resources, FAQs, and support channels to address any questions or technical difficulties.

6. **Encourage feedback:**

   Create a feedback mechanism for employees to share their thoughts, concerns, and suggestions. Actively listen to their feedback and address any valid concerns promptly. This will demonstrate that their input is valued and help foster a positive transition.

"Explaining to employees and simply articulating the BYOD strategy is pivotal. It's important to instill confidence that employees' personal privacy will remain respected while the process is underway. Being transparent and open to questions and concerns resonates well with people and eases their reluctance to join your BYOD program."

– Andrew Hutchinson – CISO, Vanderbilt University Medical Center

How will a Balanced BYOD Program Benefit my Business?

A balanced BYOD program should enable users rather than control them

Enabling BYOD for your business requires thought, planning, and hard work, but ultimately the program should end up being more than worth the effort.

Intune BYOD enabled businesses enjoy these benefits:

- Cost savings with less hardware procurement
- Have better employee productivity as their team is able to work from anywhere
- Develop a stronger security posture that is less prone to breach
- Happy Employees - satisfied with privacy and security of personal devices

A balanced BYOD Program Prevents:

- Shadow IT
- Mistrust from employees pertaining to the privacy of devices.
- Breach and data loss incidents
- Employees obligated to carry multiple devices
- Exploitation of vulnerabilities to gain unauthorized access to company resources

Implementing a Balanced BYOD Program with Intune

Why we recommend using Intune for BYOD:

Many businesses already leverage Microsoft 365 which includes Intune.
If this sounds like you, you are off to a head start as Intune is the industry leader for BYO devices. Intune enables companies to achieve a unique balance between company security and employee privacy.

Your Microsoft 365 licenses include conditional access policies, app protection policies, company portal and a phish resistant MFA solution. Combining some, or all of these controls, means you can secure data on BYO devices at no additional cost.

Gartner Magic Quadrant for Endpoint Management

Get It Right The First Time

Avoid costly errors and unintended consequences by engaging an experienced partner like Mobile Mentor to deploy your BYOD solution.

There are no short cuts, and getting it right the first time will require a 3 step process:

1. Develop a BYOD policy that balances privacy and security
2. Design the technical controls for a tiered trust model
3. Explicitly address privacy in your rollout and communications

The result is an **elegant BYOD program** that meets the needs of your business' security requirements and your employee's privacy concerns.

Your Future BYOD Program

Are You Ready?

What are you waiting for?

Are you already using Microsoft 365? If so, our BYOD 365 will give you the ability to secure company data on personal devices while simultaneously providing the privacy your employees deserve. For a free consultation, apply here.

Mobile Mentor is a global leader in the endpoint ecosystem and Microsoft's 2021 Partner of the Year in Modern Endpoint Management. Certified by Microsoft, Apple and Google, our engineers specialize in designs that balance endpoint security with employee experience for our clients. Check out our other whitepapers.

USA	+1 877 707 3848
New Zealand	+64 9 888 0512
Australia	+61 2 9575 4827

mobile-mentor.com

mobile mentor