

WHAT INSURANCE AGENCIES NEED TO KNOW ABOUT BYOD (BRING YOUR OWN DEVICE)



The Bring Your Own Device (BYOD) model is gaining traction among insurance agencies looking to enhance flexibility and reduce costs. However, carefully navigating the complexities of BYOD is crucial to ensuring data security and regulatory compliance.

Conversations around BYOD typically assume that the computers (desktops and laptops) are owned by the agency. It's best practice that the BYOD strategy focuses only on employee-owned mobile devices, such as smartphones and tablets.

This infographic explores essential insights your insurance agency needs to understand about BYOD, including its benefits and potential risks. We'll also explore the role that Mobile Device Management (MDM) and Mobile Application Management (MAM) play in implementing BYOD successfully in your agency.

BYOD

PROS



- **Cost Savings:** Not needing to purchase, maintain, and upgrade employee devices will save your agency a substantial amount of money and resources necessary for procurement.
- **Increased Productivity & Collaboration:** Your employees will be more comfortable and proficient using their personal devices, allowing them to more easily collaborate from anywhere.
- **Employee Satisfaction:** Your employees can work from anywhere, giving them a sense of autonomy and flexibility.
- **Scalability:** Rather than purchasing new devices for new employees, they can use their own devices as long as they meet security requirements.

CONS



- **Increased Security Risks:** BYOD increases the risk of security breaches, as personal devices are more difficult to control and monitor.
- **Regulatory Compliance:** Ensuring compliance with data protection regulations can be more challenging, as personal devices may not meet the required security standards.
- **IT Management Complexity:** Managing a variety of different devices and operating systems can complicate IT operations, including the implementation of security policies and the provisioning of support.
- **Legal and Privacy Concerns:** There are potential legal implications regarding employee privacy, especially if the company needs to access a device to investigate a security incident or retrieve company data.

MUST-HAVES FOR IMPLEMENTING BYOD IN YOUR AGENCY



CLEARLY ESTABLISHED BYOD POLICY



SUPPORT & RESOURCES



REGULAR MONITORING AND REPORTING



SECURITY AWARENESS TRAINING



ROBUST SECURITY MEASURES



MOBILE DEVICE & APPLICATION MANAGEMENT

UNDERSTANDING MOBILE APPLICATION MANAGEMENT (MAM) AND MOBILE DEVICE MANAGEMENT (MDM)

MOBILE APPLICATION MANAGEMENT MAM

VS

MOBILE DEVICE MANAGEMENT MDM

- | | |
|---|--|
| <ul style="list-style-type: none"> ✓ Maintains privacy and flexibility while outlining specific security requirements ✓ Best for personal devices that access company resources (BYOD) ✓ IT controls access to company data through specific applications ✓ IT does not control the device, or have access to any of the personal information on the device | <ul style="list-style-type: none"> ✓ Prioritizes security over privacy and flexibility ✓ Best for corporate devices ✓ IT has total control of the device and the data ✓ IT can lock and/or reset devices that are lost or stolen |
|---|--|

MICROSOFT 365 BRING-YOUR-OWN-DEVICE (BYOD) OPTIONS

Microsoft 365 offers a suite of tools and features that can help your agency implement and manage a BYOD strategy. By default, any device can access your Corporate Microsoft 365 resources. While this is very convenient, it is not very secure, as it exposes your agency to significantly higher risk.

With Microsoft 365, you can implement policies that manage personal device access and help to reduce security risks such as those associated with loss, theft, or other compromise.

Four Options for Managing BYOD Risks

- 1 **MAM:** This management option lets you control application data, enforce device PINs, encrypt stored data, and prevent data leakage. But it doesn't protect against malware or cyber threats.
- 2 **MDM:** With this option, you gain enhanced device oversight and security. You can also block non-compliant devices from accessing business apps and data and enforce policies to mitigate malware and cyber threats.
- 3 **Limited Web Access:** Devices are not managed at all, though Microsoft 365 app usage is limited, and users are prevented from downloading, printing, or syncing data.
- 4 **No Access:** You can choose to block personal device access outright.

		ACCESSIBILITY			
		CLIENT APP ACCESS	WEB ONLY	NO ACCESS	
MANAGEMENT		Option 1 MAM	Option 2 MDM	Option 3 Limited Web Access	Option 4 No Access
SECURITY POLICIES		Multi-Factor Authentication	Enforce Device Compliance	Block download, print, and sync	Block all access on personal devices
DEVICE POLICIES		<ul style="list-style-type: none"> ✓ Encrypt App data ✓ Require PIN ✓ Prevent leakage ✓ Remote wipe 	<ul style="list-style-type: none"> ✓ Encrypt App data ✓ Require PIN ✓ Prevent leakage ✓ Remote wipe ✓ Device Health ✓ Defender policies 	Devices will not be managed if no data is allowed on the device	
		← Flexible		Secure →	

This resource has been made available to you by **Kite Technology Group and Agents Council for Technology.**

We hope that this infographic helps provide an overview of how insurance agencies can effectively implement a Bring Your Own Device (BYOD) policy, highlighting the crucial roles of Mobile Device Management (MDM) and Mobile Application Management (MAM) in maintaining security and compliance.



[WWW.KITECHGROUP.COM](http://www.kitechgroup.com)



[WWW.INDEPENDENTAGENT.COM/ACT](http://www.independentagent.com/act)

