

RISK & COMPLIANCE

Chris Brewer & Alyssa Pugh

When Business is Personal: A Chat about MDM & BYOD



1

DISCLAIMER

- **This presentation is for information only.**
Evaluate risks before acting based on ideas from this presentation.
- **This presentation contains the opinions of the presenters.**
Opinions may not reflect the opinions of Tandem.
- **This presentation is proprietary.**
Unauthorized release of this information is prohibited.
Original material is copyright © 2024 Tandem.



2



Alyssa Pugh

CISM, Security+
Tandem | GRC Content Manager



Chris Brewer

VCP
CoNetrix Technology | Team Lead



3

Agenda

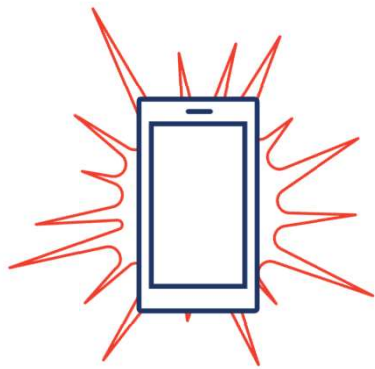
WHEN BUSINESS IS PERSONAL: A CHAT ABOUT MDM & BYOD

- Mobile Devices
- Bring Your Own Device (BYOD)
- Mobile Device Management (MDM)
 - Regulatory Guidance
 - Administrative Controls
 - Technical Controls
- Frequently Asked Question
- Key Takeaways

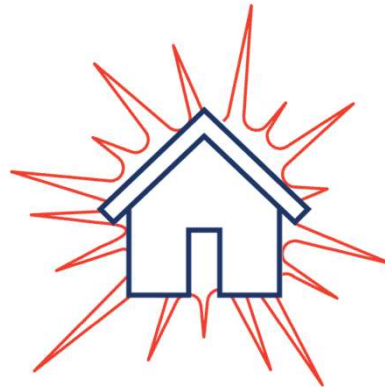


4

Why MDM & BYOD?



Mobile Device Explosion



Remote Work Explosion



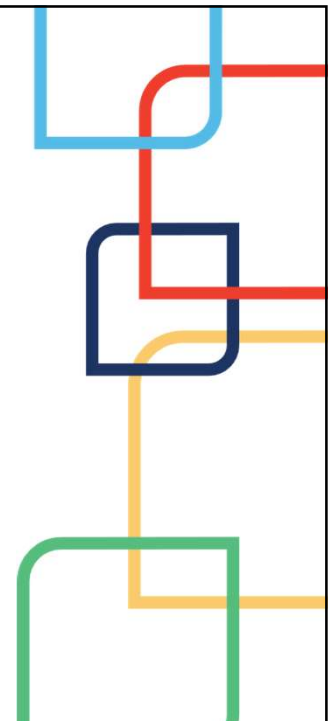
5

RISK & COMPLIANCE


Chris Brewer & Alyssa Pugh

When Business is Personal: A Chat about MDM & BYOD

& protecting your data



6




Mobile Devices

WHEN BUSINESS IS PERSONAL: A CHAT ABOUT MDM & BYOD

7

POLL QUESTION

How many mobile devices do you actively use?



8

What is a “mobile device?”

NIST & FFIEC DEFINITION

“A portable computing device that:

1. Has a small form factor such that it can easily be carried by a single individual;
2. Is designed to operate without a physical connection (e.g., wirelessly transmit or receive information);
3. Possesses local, non-removable data storage;
4. Is powered-on for extended periods of time with a self-contained power source.”

1. Small
2. Wireless
3. Local Storage
4. Battery-Powered



9

Mobile Devices



10

QUESTION

What mobile devices do I need to manage?

ANSWER

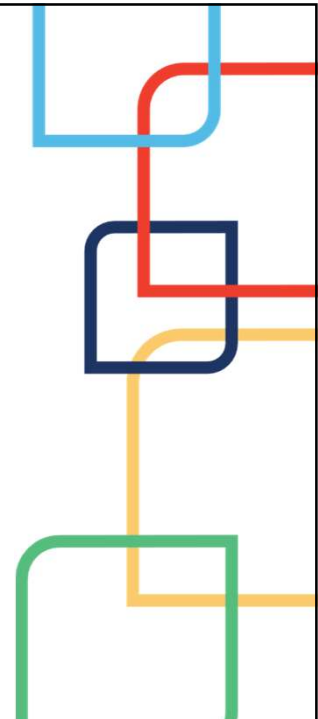
The ones where your data is at the greatest risk of being compromised.



11

Bring Your Own Device (BYOD) vs. Company-Owned Devices

WHEN BUSINESS IS PERSONAL: A CHAT ABOUT MDM & BYOD



12

DISCUSSION TOPIC

Do you use your personal mobile devices for business purposes?



13

Personal Devices for Work

Remote Access



Email & Calendar



Team Collaboration



Security Systems & Multifactor Authentication




Productivity & Project Management



14

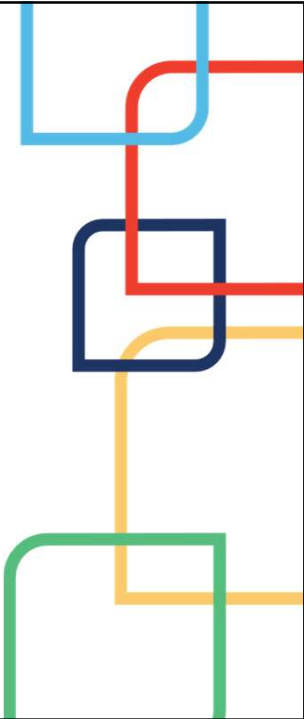
	BYOD	COMPANY-OWNED
Security	-	+
Compliance	-	+
Management	-	+
Autonomy	+	-
Privacy	+	-
Cost	+	-



15

Mobile Device Management (MDM)

WHEN BUSINESS IS PERSONAL: A CHAT ABOUT MDM & BYOD



16

Regulatory Guidance

FFIEC Information Security Booklet | II.C.15(d) Use of Remote Devices



Administrative Controls

- Business Case
- Management Approval
- Regular Access Review
- Assurance & Testing*
- Policies & Procedures (Page 26)
- Training (Page 29)

Technical Controls

- Access Controls
- Anti-Malware
- Authentication
- Baselines & Configurations*
- Encryption
- Patch Management
- Log Management
- Remote Wipe*

* For company-owned devices

<https://ithandbook.ffiec.gov/it-booklets/information-security/>



17

Regulatory Guidance

Additional FFIEC Recommendations



Device / Endpoint Security Component

IV.B Communications
V. Business Continuity Plan

III.B IT Asset Management

https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf
https://ithandbook.ffiec.gov/media/2nifgh2b/ffiec_itbooklet_businesscontinuitymanagement_v3.pdf
https://ithandbook.ffiec.gov/media/ywfm2ftz/ffiec_itbooklet_aio.pdf



18

Regulatory Guidance



NIST CYBERSECURITY FRAMEWORK 2.0

“The Functions, Categories, and Subcategories apply [...] to all types of technology environments, including cloud, **mobile**, and artificial intelligence systems.”

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST_CSWP_29.pdf



19

Regulatory Guidance Takeaways

1

Key controls are key for a reason.

2

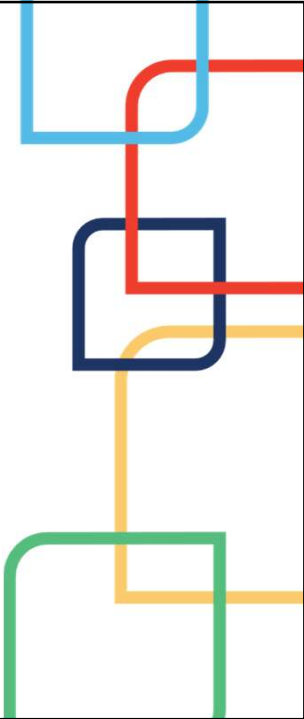
A silver bullet solution does not exist.



20




MDM Administrative Controls


WHEN BUSINESS IS PERSONAL: A CHAT ABOUT MDM & BYOD



21

Administrative Controls

<h3>Training</h3> 	<h3>Offboarding</h3> 	<h3>Documents</h3> 
---	--	--



22

Administrative Controls: Training

1

Train on what mobile devices employees can and can't use.

2

Train on how to physically protect mobile devices.

3

Train on how to technically protect mobile devices.



23

Security Awareness Training (v7.0)

TECHNICAL SECURITY

Lock Your Devices

When you use a mobile device for work, **turn on the passcode and/or biometrics** to unlock it. Also, when you leave a device for any amount of time, even in a secure location, **lock or sign out of your account**. This way, if someone gets the device, it is much more difficult for the person to access your data.

Lessons 3/8

- Physical Security (v7.0)
 - About Physical Security
 - Secure Your Paper Data
 - Secure Your Laptop
 - Secure Your Devices
 - Secure Your Screens
 - Question 1
 - Question 2
 - Question 3
 - Question 4
- Technical Security (v7.0)**
 - Technical Security
 - Use Cybersecurity Features

← Back Next → Slide 20 of 78 Save & Close

Tandem

24

Administrative Controls: Offboarding

1

Remove Access

2

Risk Assess

3

Reclaim Assets



25

Administrative Controls: Documents



Mobile Device
Management Policy



Acceptable Use
Policy / Agreement



Nondisclosure
Agreement (NDA)




26

Related Policies

Related Policy	Description
Data M	
Emplo Aware	
Inciden	Mobile Device Management (MDM)
IT Asse	Revision 1.0
Person	Approval Pending
Remon	Securely provision, monitor, and manage mobile devices used for business purposes. Prohibit the use of unauthorized mobile devices.
Secur	Commentary
System	The National Institute of Standards and Technology (NIST) defines a "mobile device" as: "A portable computing device that (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connector (e.g., wireless transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source."
User A	For the purpose of this policy, the following items are considered to be "mobile devices."
Vulner Manage	<ul style="list-style-type: none"> Laptops Phones (e.g., smartphones, cellphones, etc.) Tablets Wearables (e.g., smartwatches, smart glasses, etc.) Other portable devices (e.g., e-readers, digital assistants, navigation devices, digital cameras, etc.)
Commi	The use of mobile devices for business purposes is becoming more common due to technological advancements and operational efficiencies. Some examples of mobile device use for business purposes could include, but are not limited to:
Emplo	<ul style="list-style-type: none"> Connecting to the organization's network from a remote location (a.k.a., "remote access"). Performing remote processing functions. Building resilience into business continuity objectives. Accessing, storing, or transmitting organization or customer information. Using work communication channels, like email, team collaboration tools, video conferencing, or file sharing.
Quar	To promote security, the organization needs to ensure effective mobile device controls are in place, and users are educated on security expectations.
Quar	At times, personnel may wish to use a personally-owned device to perform work-related duties. This is commonly referred to as "bring your own device" or "BYOD." If the organization elects to allow BYOD, the same security requirements for both organization-owned and personally-owned mobile devices should be enforced. BYOD
Similar	
Similar	

TEMPLATE POLICY


Tandem.App/KEYS-MDM-Policy



27

MDM Technical Controls

WHEN BUSINESS IS PERSONAL: A CHAT ABOUT MDM & BYOD



28

Technical Controls

**MDM / MAM
Systems**



**App Protection
Policies**



**Conditional
Access**




29

Learn Discover Product documentation Development languages Topics Sign in


Microsoft Intune Product documentation Learn Intune Developer resources Troubleshooting Resources Portal Free account

Microsoft Intune documentation


Official product documentation for Microsoft Intune




OVERVIEW
[What is Intune?](#)



OVERVIEW
[What's new in Intune](#)



OVERVIEW
[Features in development](#)



OVERVIEW
[Microsoft Intune Suite add-ons](#)

<https://learn.microsoft.com/en-us/mem/intune/>

30

MDM / MAM Systems

 Microsoft Intune

 mobileiron

 airwatch
by vmware

 ManageEngine

 CITRIX
XenMobile




31

DISCUSSION TOPIC

Do you use an MDM / MAM system?
If so, what do you use?



32



	MDM	MAM
Scope	Control of entire device	Control of specific apps
Policy Enforcement	Configuration, updates, and security of entire device	Configuration, updates, and security of specific apps
Remote Wiping	Full device	Limited to specific apps
User Privacy	More invasive	Less invasive
Deployment	Better for company-owned devices	Better for BYOD

33

App Protection Policies

LEVEL 1

Enterprise Basic
Data Protection


LEVEL 2

Enterprise Enhanced
Data Protection

LEVEL 3

Enterprise High
Data Protection

<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-outlook>



34


INTUNE EXAMPLE

✓ Basics
✓ Apps
3 Data protection
4 Access requirements
5 Conditional launch
6 Assign

This group includes the Data Loss Prevention (DLP) controls, like cut, copy, paste, and save-as restrictions. These settings determine how users interact with data in the apps.

Data Transfer

Backup org data to iTunes and iCloud backups ⓘ	<input type="radio"/> Allow <input checked="" type="radio"/> Block
Send org data to other apps ⓘ	<input type="text" value="Policy managed apps with Open-In/Share filtering"/>
Select apps to exempt	<input type="button" value="Select"/>
Select universal links to exempt	<input type="button" value="Select"/>
Select managed universal links	<input type="button" value="Select"/>
Save copies of org data ⓘ	<input type="radio"/> Allow <input checked="" type="radio"/> Block
Allow user to save copies to selected services ⓘ	<input type="text" value="OneDrive for Business"/>




35

INTUNE EXAMPLE

✓ Basics
✓ Apps
✓ Data protection
4 Access requirements
5 Conditional launch
6 Assign

Configure the PIN and credential requirements that users must meet to access apps in a work context.

PIN for access ⓘ	<input checked="" type="radio"/> Require <input type="radio"/> Not required
PIN type ⓘ	<input checked="" type="radio"/> Numeric <input type="radio"/> Passcode
Simple PIN ⓘ	<input type="radio"/> Allow <input checked="" type="radio"/> Block
Select minimum PIN length ⓘ	<input type="text" value="6"/>
Touch ID instead of PIN for access (iOS 8+/iPadOS) ⓘ	<input checked="" type="radio"/> Allow <input type="radio"/> Block
Override biometrics with PIN after timeout ⓘ	<input checked="" type="radio"/> Require <input type="radio"/> Not required
Timeout (minutes of inactivity) *	<input type="text" value="30"/> ✓
Face ID instead of PIN for access (iOS 11+/iPadOS) ⓘ	<input checked="" type="radio"/> Allow <input type="radio"/> Block



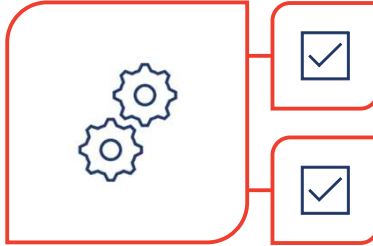
36

Example: Conditional Access

Applies to iOS and Android Devices



Block Exchange
ActiveSync



Allow Access

Approved Client Apps

App Protection Policy

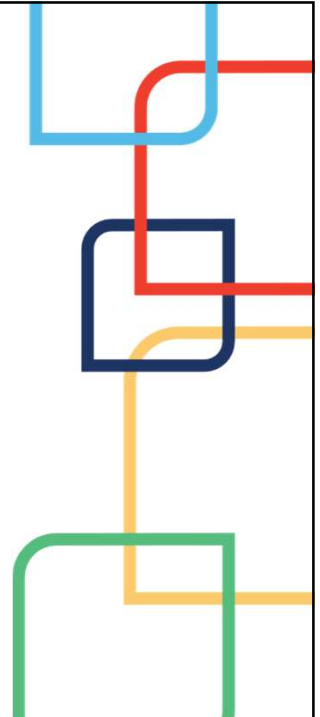
<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-outlook>
<https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-policy-approved-app-or-app-protection>



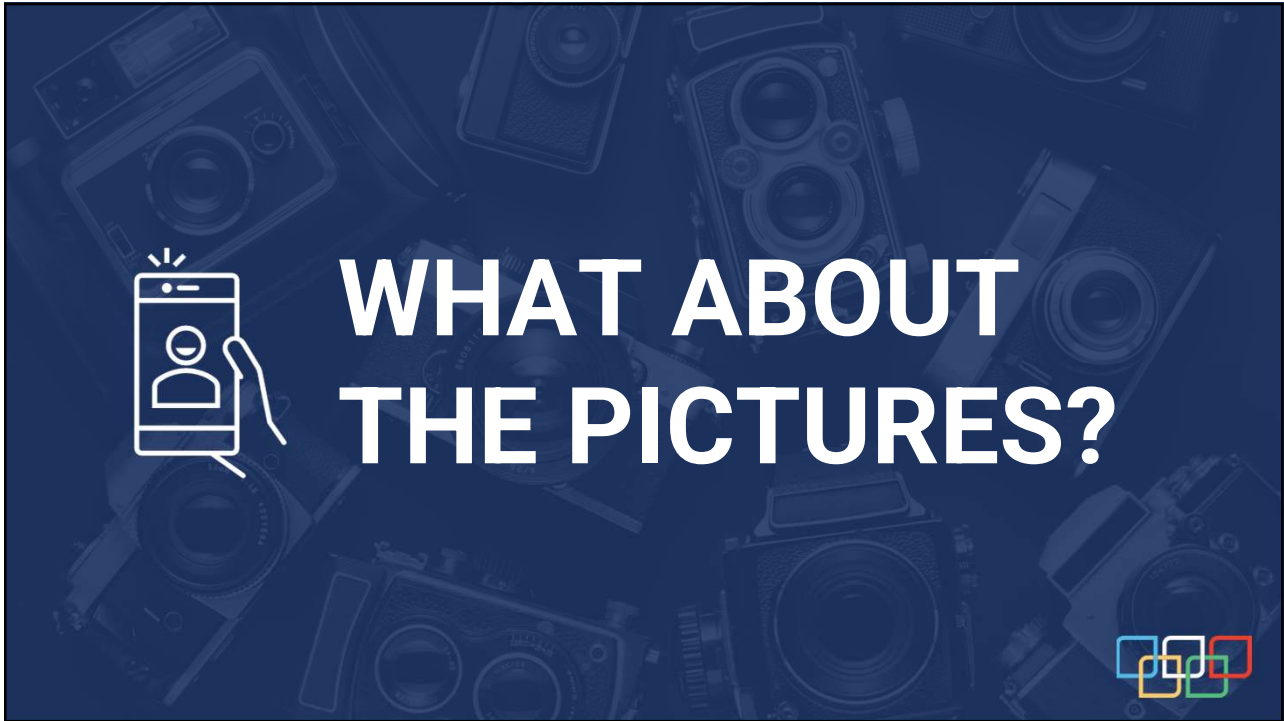
37

Frequently Asked Question

WHEN BUSINESS IS PERSONAL: A CHAT ABOUT MDM & BYOD



38



39



40

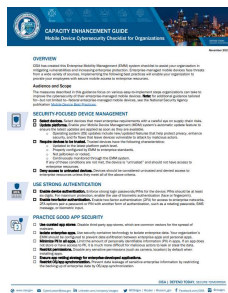
Key Takeaways

- 1 You do mobile device management to protect your data.
- 2 There is no one “right” solution for mobile device management.
- 3 Find the balance between functionality, efficiency, and security.
- 4 Manage risk holistically with technical *and* administrative controls.

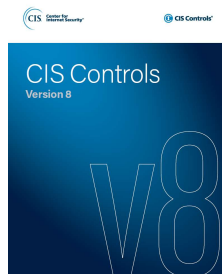


41

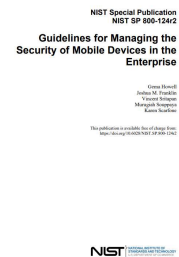
Other Resources



CISA Mobile Device Cybersecurity Checklists



CIS Controls v8



NIST SP800-124r2

<https://www.cisecurity.org/controls/v8>
<https://csrc.nist.gov/pubs/sp/800/124/r2/final>
<https://www.cisa.gov/news-events/alerts/2021/11/24/cisa-releases-capacity-enhancement-guides-enhance-mobile-device>



42



43

THANKS FOR JOINING!

When Business is Personal: A Chat about MDM & BYOD

<p>Chris Brewer CoNetrix Technology Team Lead cbrewer@conetrix.com LinkedIn.com/in/TheChrisBrewer</p>	<p>Alyssa Pugh Tandem GRC Content Manager apugh@tandem.app LinkedIn.com/in/AlyssaPugh</p>
---	---

KEYS
CONFERENCE

44