WELCOME TO

When Business is Personal: A Chat about MDM & BYOD

Chris Brewer, VCP
Team Lead
CoNetrix Technology, LLC

Alyssa Pugh, CISM, CRISC
GRC Content Manager
Tandem, LLC

Tandem

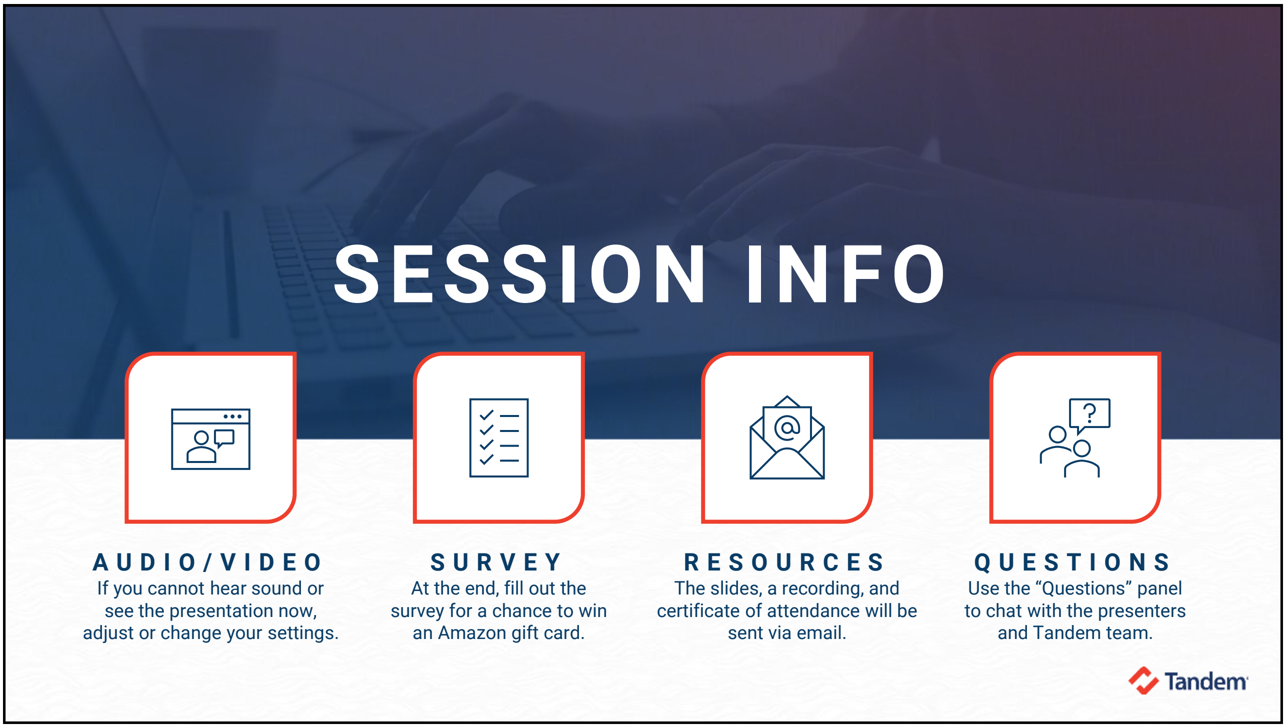
1

DISCLAIMER

- **This presentation is for information only.**
  Evaluate risks before acting on ideas from this session.
- **This presentation contains 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.

Tandem

2



SESSION INFO

AUDIO/VIDEO
If you cannot hear sound or see the presentation now, adjust or change your settings.

SURVEY
At the end, fill out the survey for a chance to win an Amazon gift card.

RESOURCES
The slides, a recording, and certificate of attendance will be sent via email.

QUESTIONS
Use the "Questions" panel to chat with the presenters and Tandem team.

Tandem

3

- Audit Management
- Business Continuity Plan
- Compliance Management
- Cybersecurity
- Identity Theft Prevention
- Incident Management
- Internet Banking Security
- Phishing
- Policies
- Risk Assessment
- Vendor Management

Tandem®
A CoNetrix company

Tandem

4

ABOUT THE SPEAKERS

Alyssa Pugh
GRC Content Manager
Tandem

Chris Brewer
Team Lead
CoNetrix Technology

Tandem

5

POLL QUESTION

What type of organization do you currently work for?

Tandem

6

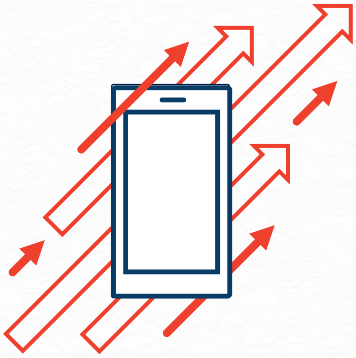
Agenda

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

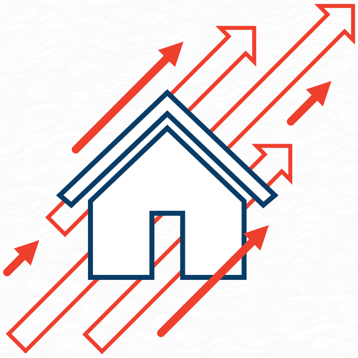
SUBMIT YOUR QUESTIONS!

7

WHY MDM & BYOD

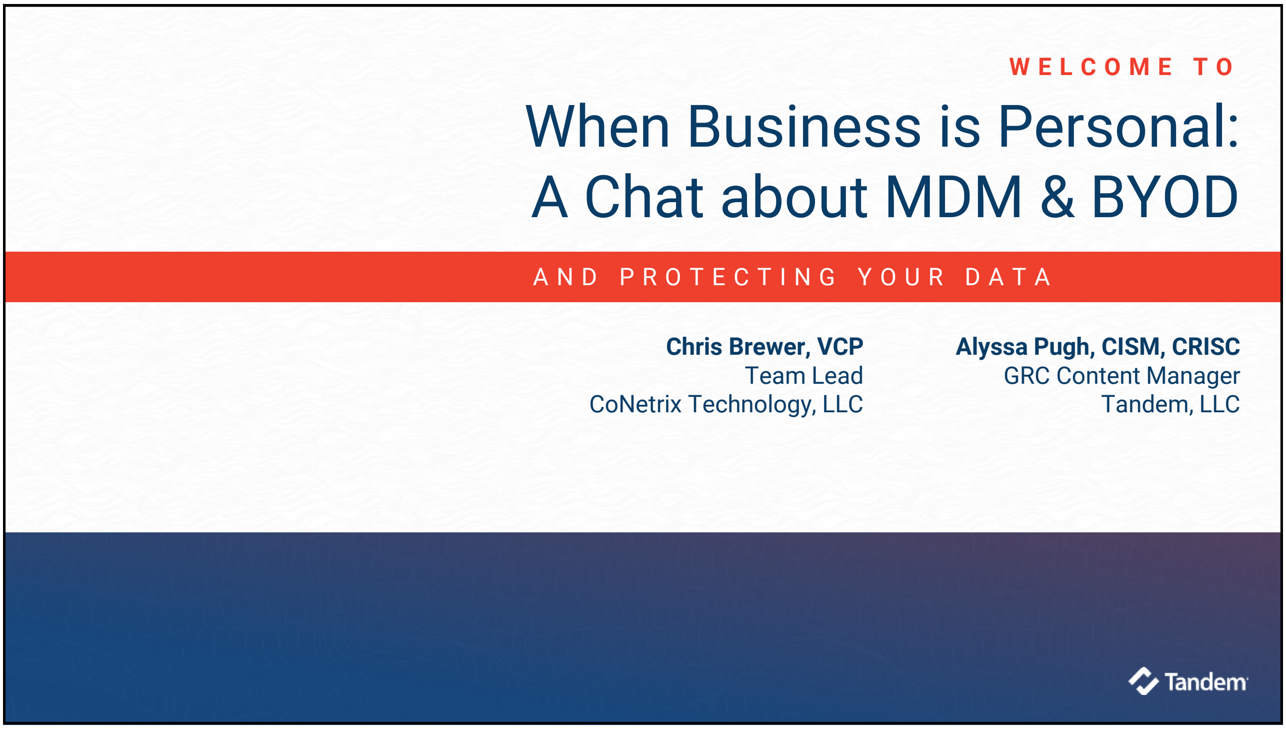


Rise of Mobile Devices



Rise of Remote Work

8



WELCOME TO

When Business is Personal: A Chat about MDM & BYOD

AND PROTECTING YOUR DATA

Chris Brewer, VCP
Team Lead
CoNetrix Technology, LLC

Alyssa Pugh, CISM, CRISC
GRC Content Manager
Tandem, LLC

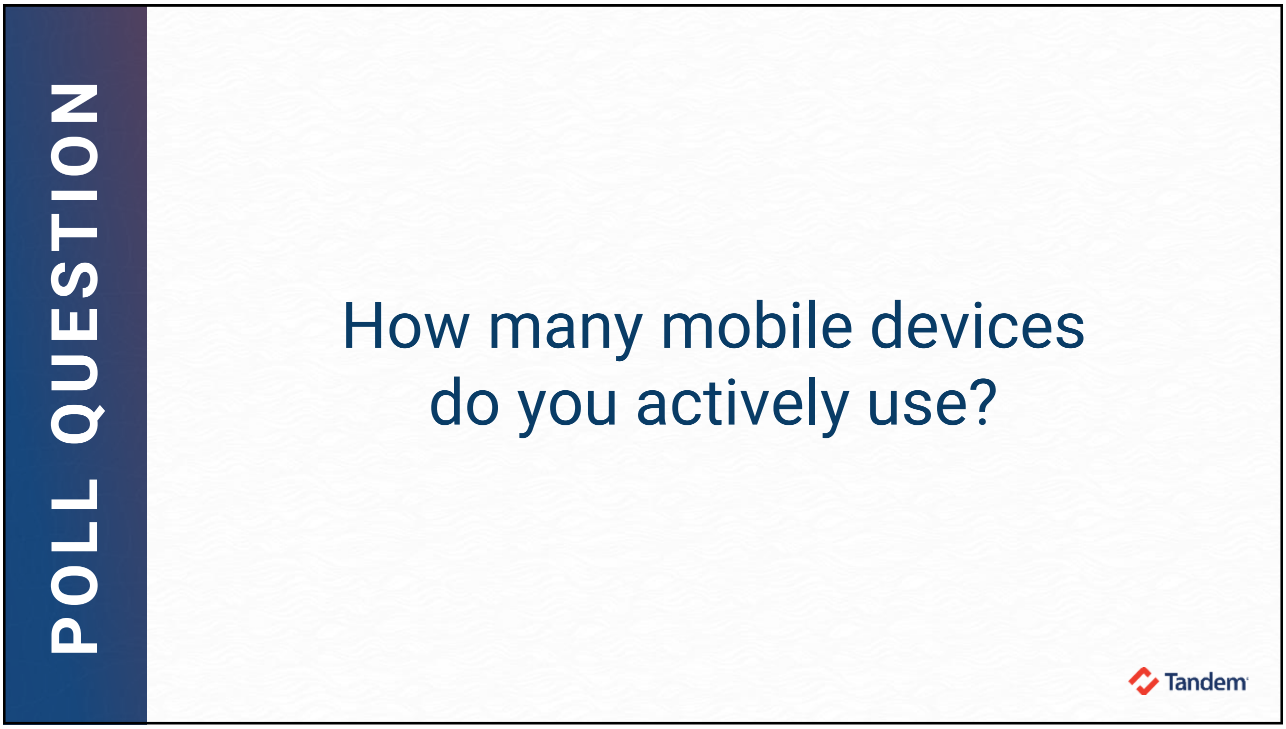
Tandem

9

Mobile Devices

Tandem

10

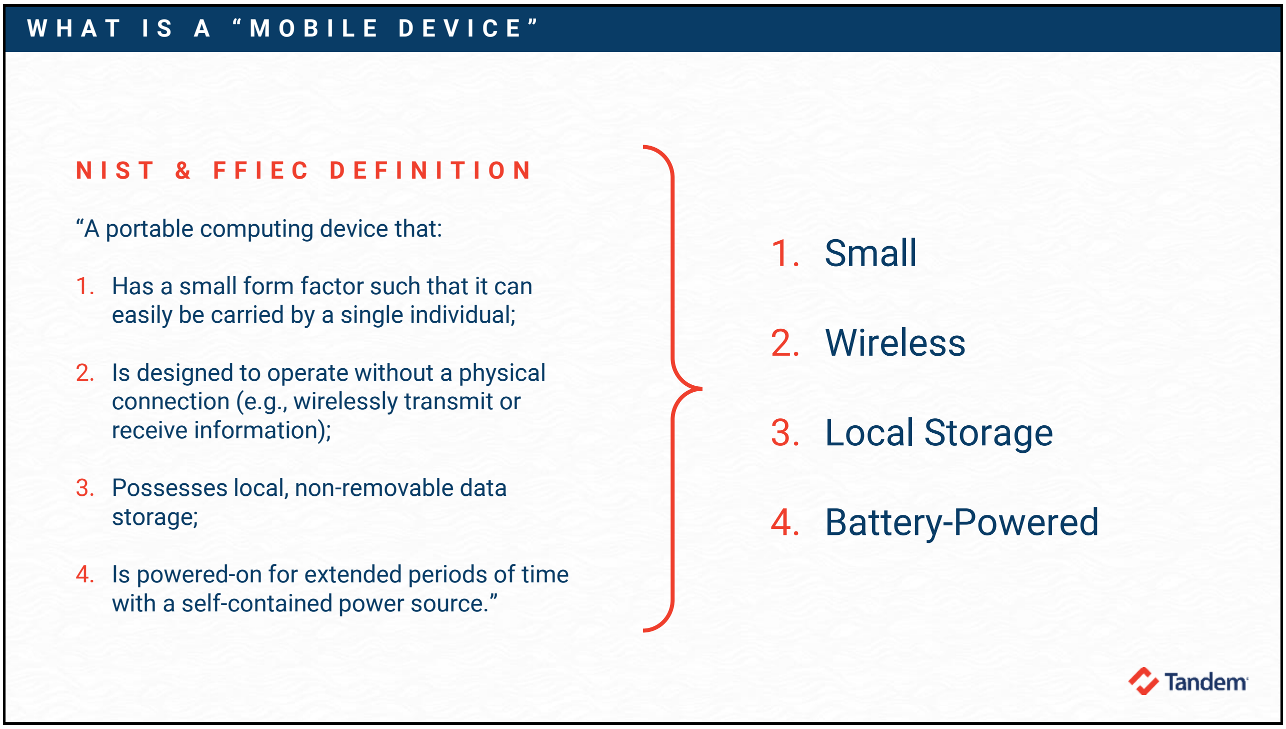


POLL QUESTION

How many mobile devices do you actively use?

Tandem

11



WHAT IS A "MOBILE DEVICE"

NIST & FFIEC DEFINITION

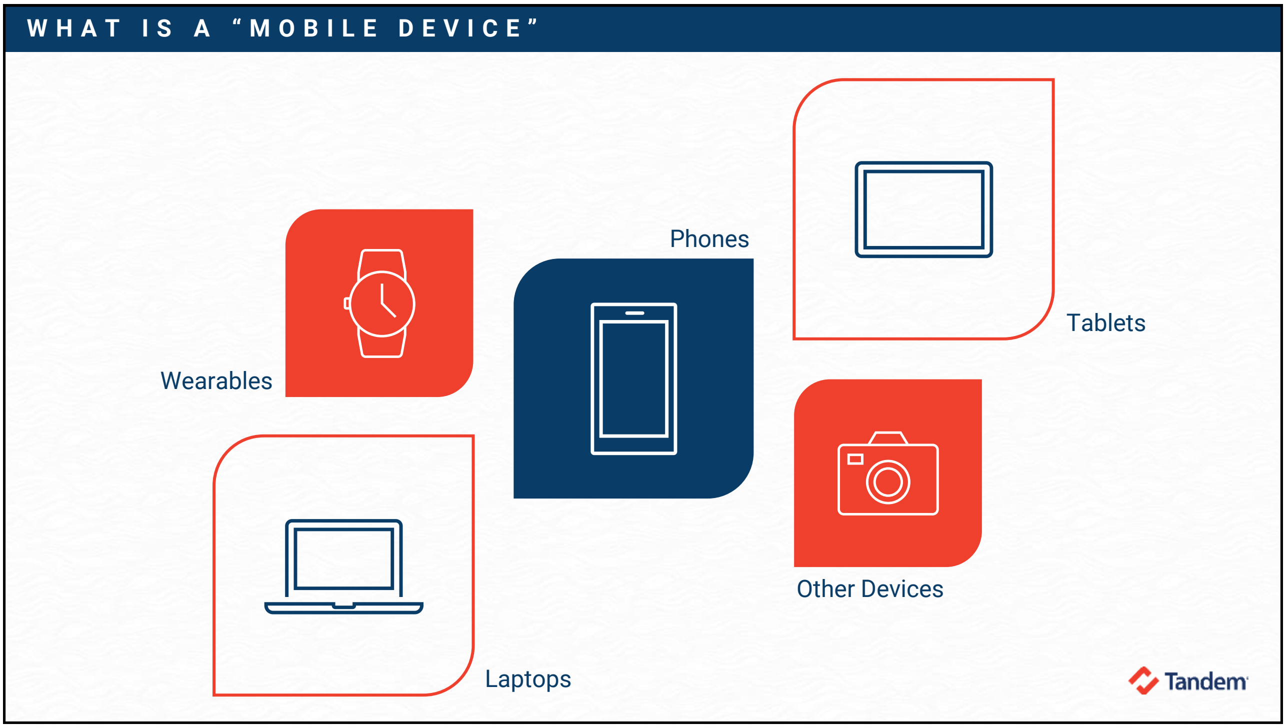
"A portable computing device that:

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

Tandem

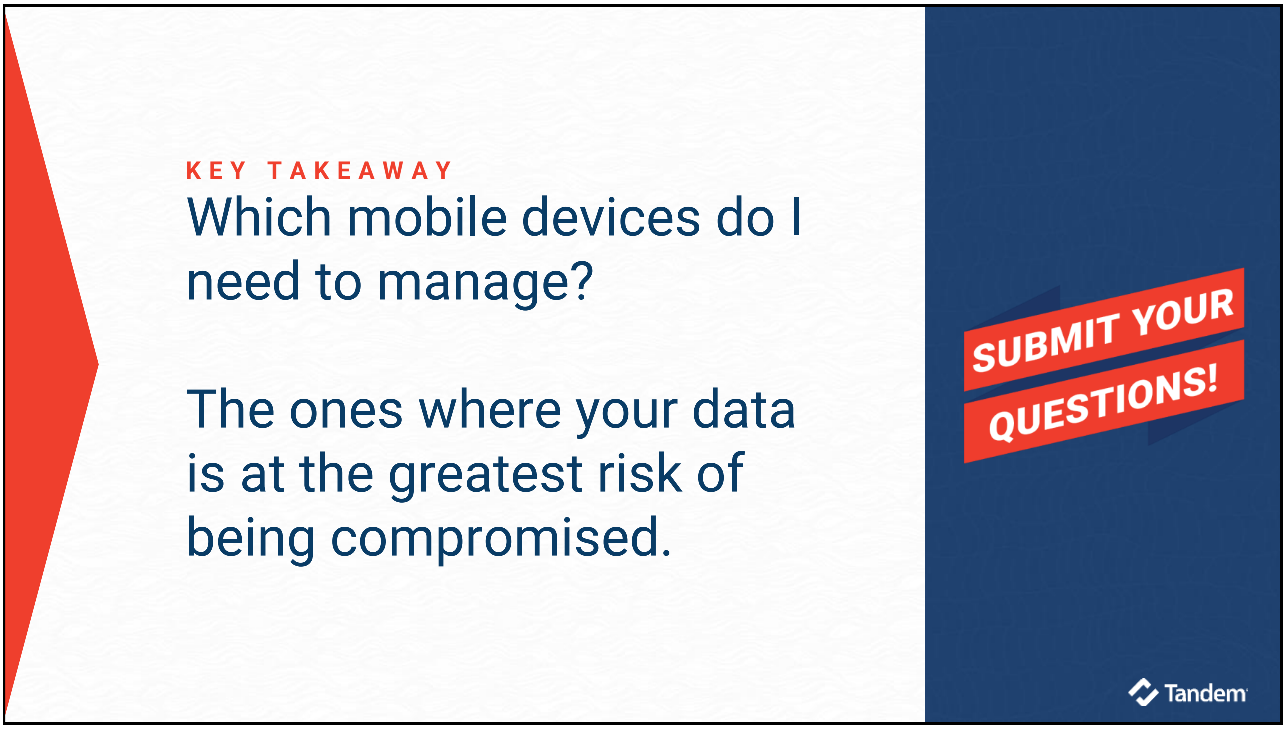
12



WHAT IS A "MOBILE DEVICE"

Phones
Tablets
Wearables
Other Devices
Laptops
Tandem

13



KEY TAKEAWAY

Which mobile devices do I need to manage?

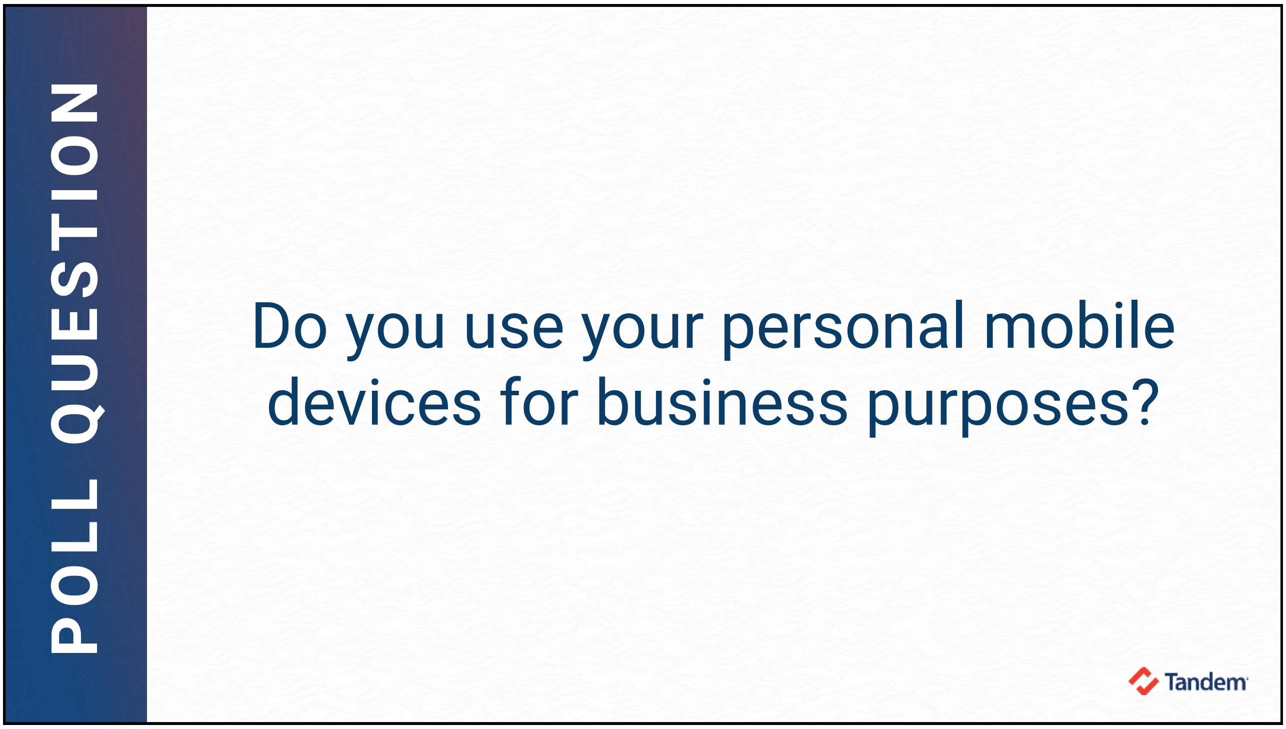
The ones where your data is at the greatest risk of being compromised.

SUBMIT YOUR QUESTIONS!

14

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

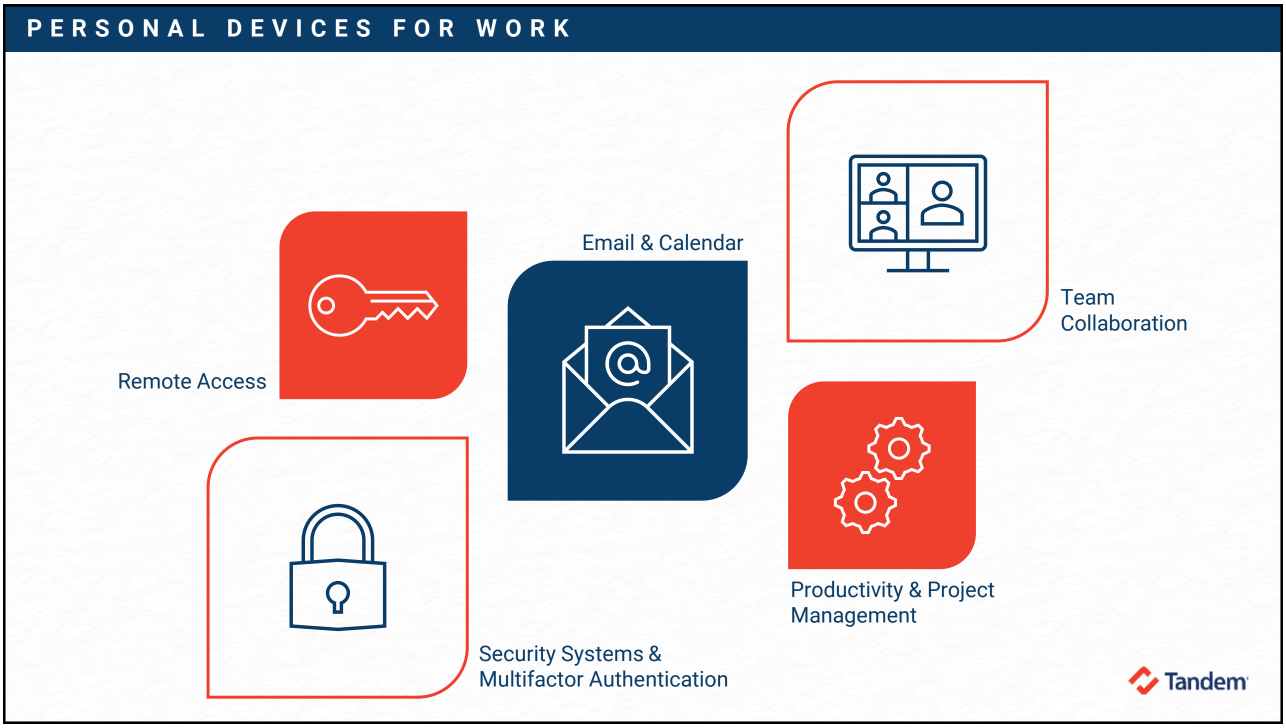
15



POLL QUESTION

Do you use your personal mobile devices for business purposes?

16



PERSONAL DEVICES FOR WORK

Remote Access

Email & Calendar

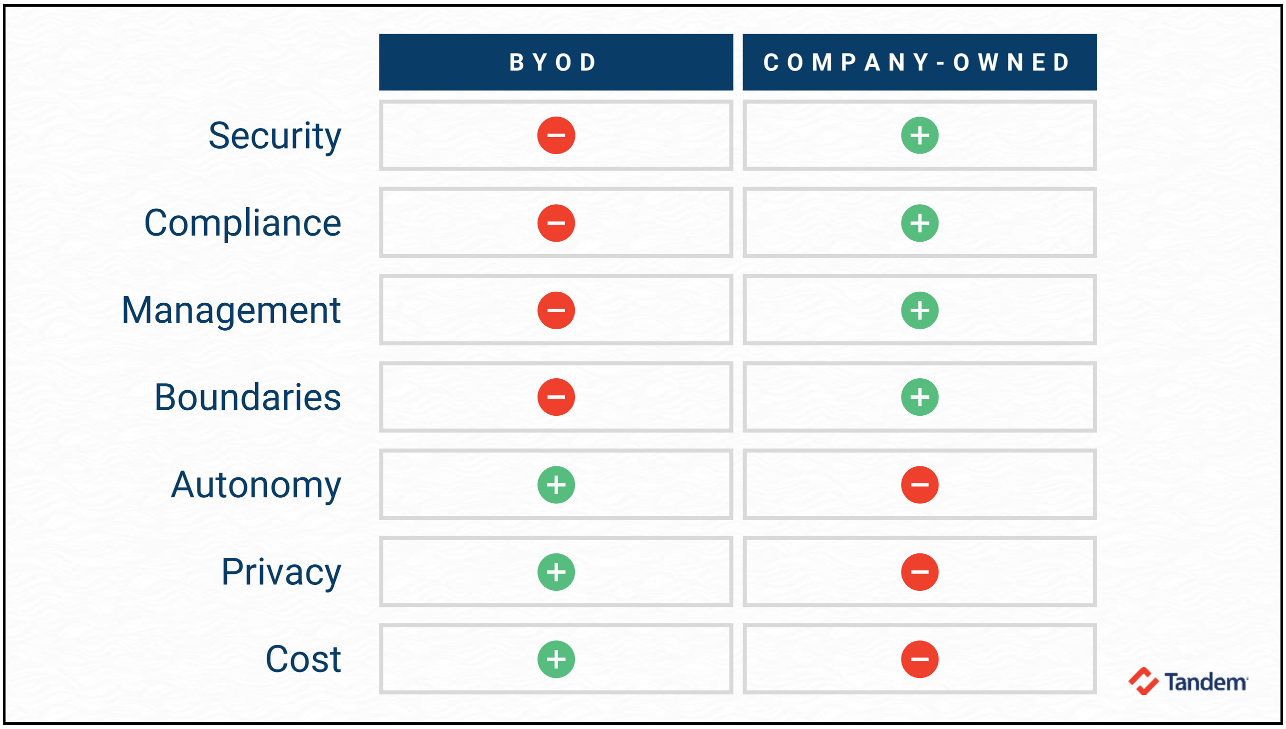
Team Collaboration

Security Systems & Multifactor Authentication

Productivity & Project Management

Tandem

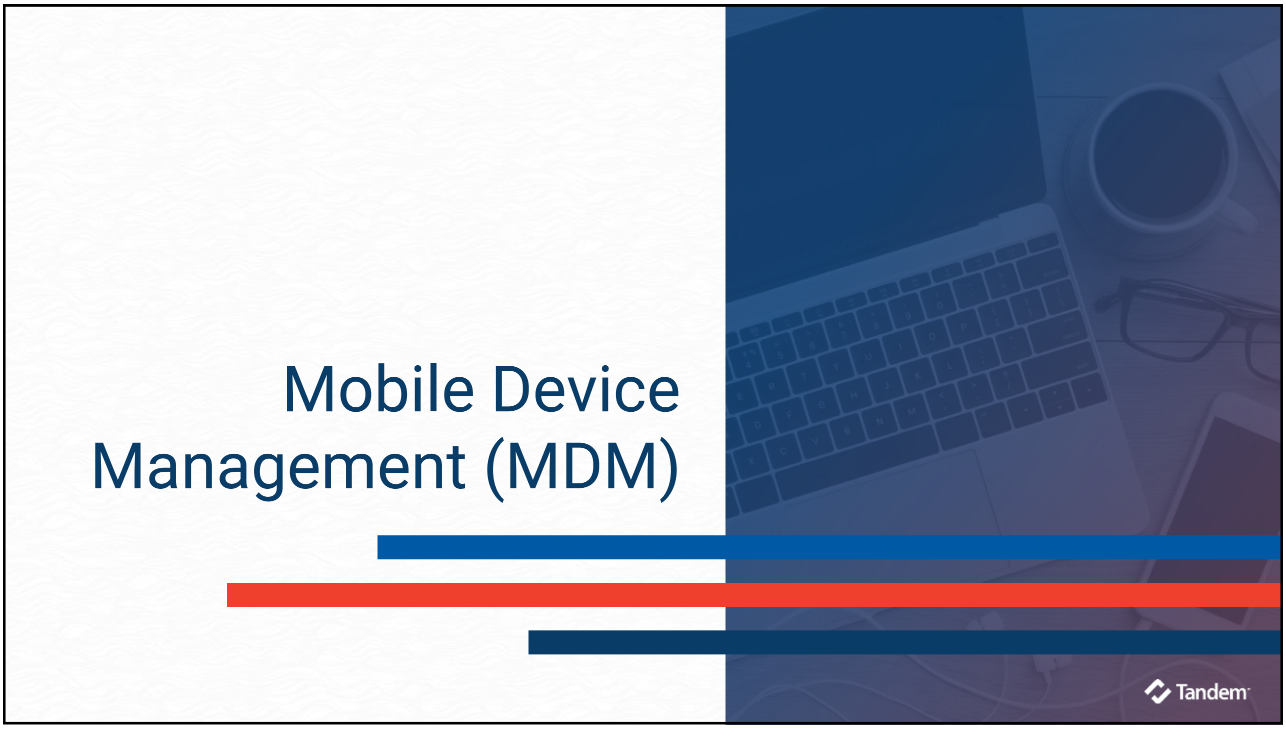
17



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

Tandem

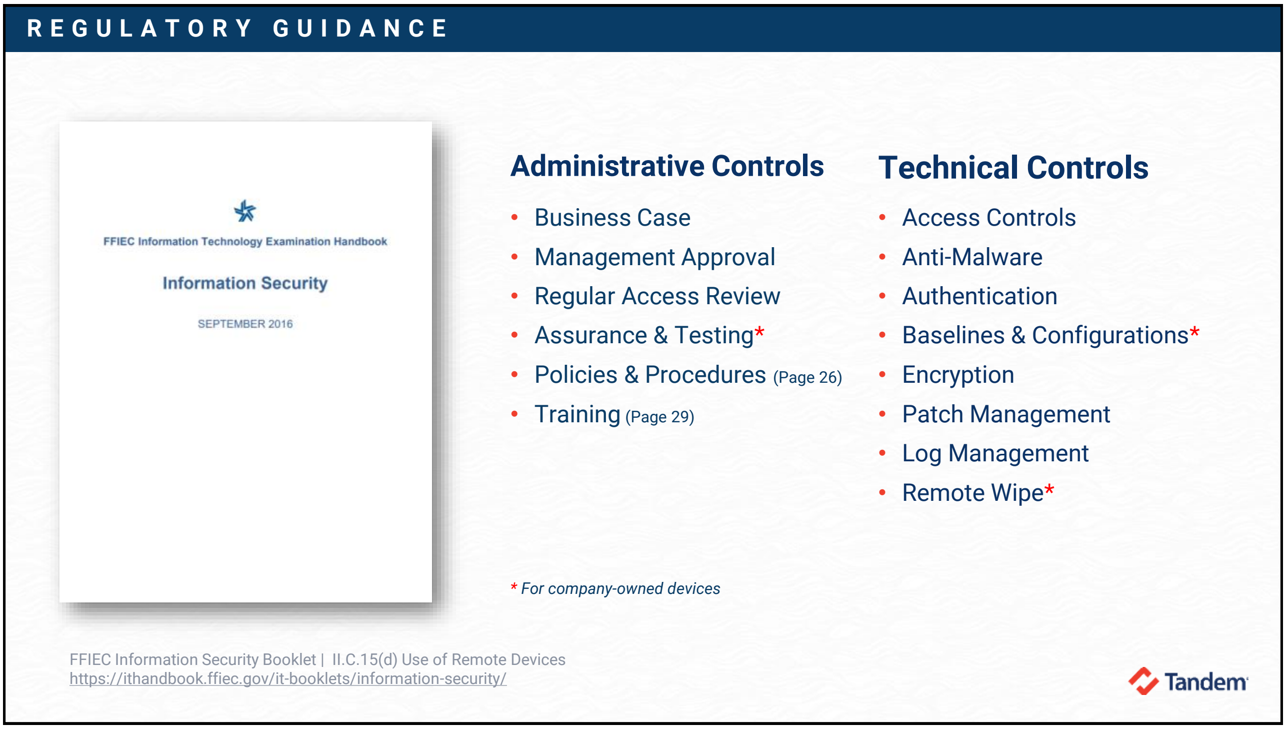
18



Mobile Device Management (MDM)

Tandem

19



REGULATORY GUIDANCE

FFIEC Information Technology Examination Handbook

Information Security

SEPTEMBER 2016

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*

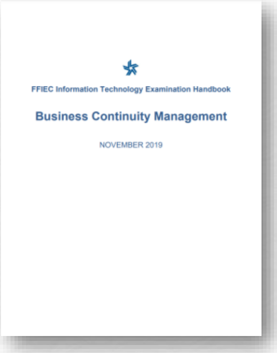
** For company-owned devices*

FFIEC Information Security Booklet | II.C.15(d) Use of Remote Devices
https://ithandbook.ffiec.gov/it-booklets/information-security/

Tandem

20

REGULATORY GUIDANCE


FFIEC Information Technology Examination Handbook

Business Continuity Management

NOVEMBER 2019

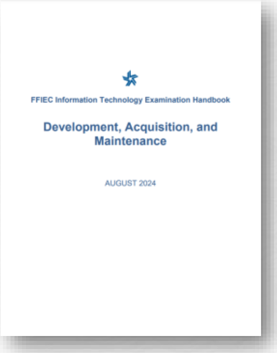
IV.B Communications
V. Business Continuity Plan

FFIEC Information Technology Examination Handbook

Architecture, Infrastructure, and Operations

JUNE 2021

III.B IT Asset Management


FFIEC Information Technology Examination Handbook

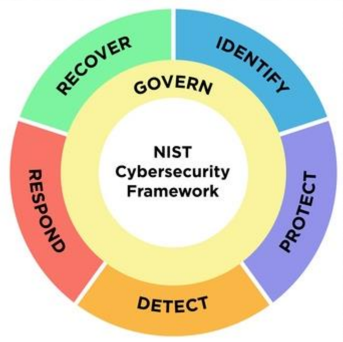
Development, Acquisition, and Maintenance

AUGUST 2024

V. Development

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

INDUSTRY GUIDANCE



NIST CSF 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

KEY TAKEAWAYS

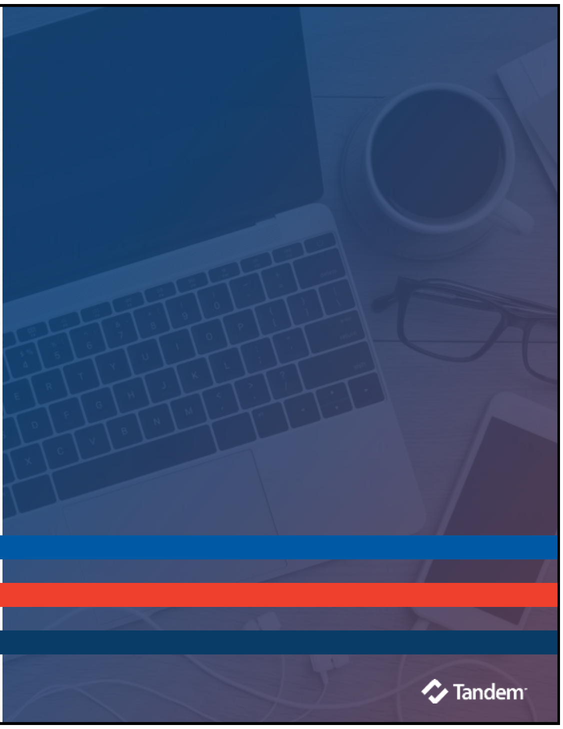
1. Key controls are key for a reason.
2. A silver bullet solution does not exist.
3. But we have to do something.

SUBMIT YOUR QUESTIONS!

Tandem

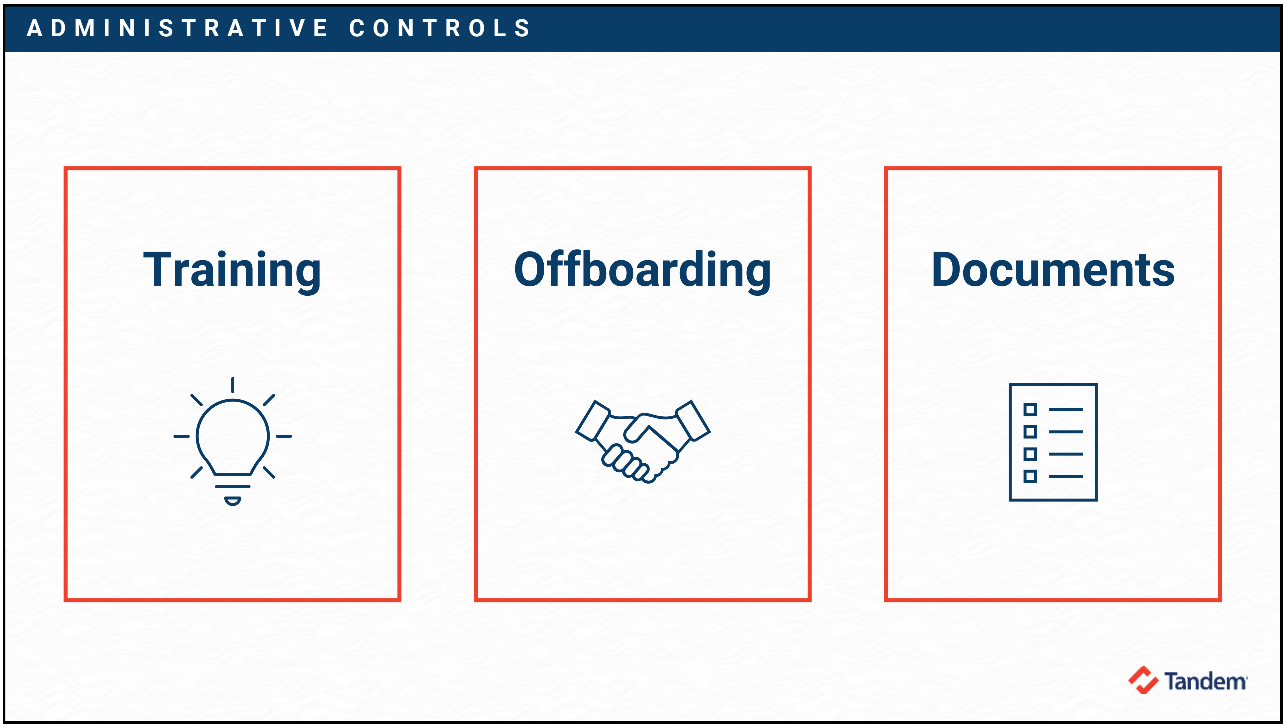
23

MDM Administrative Controls



Tandem

24



ADMINISTRATIVE CONTROLS

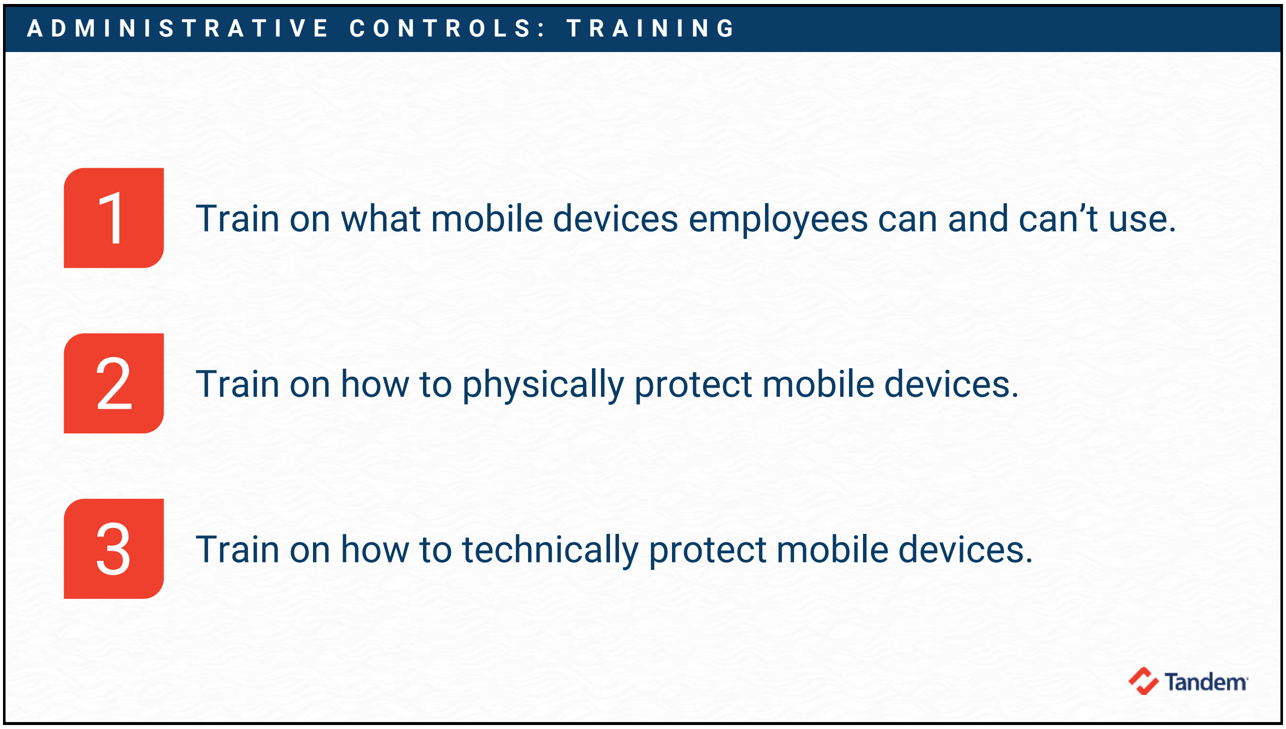
Training

Offboarding

Documents

Tandem

25



ADMINISTRATIVE CONTROLS: TRAINING

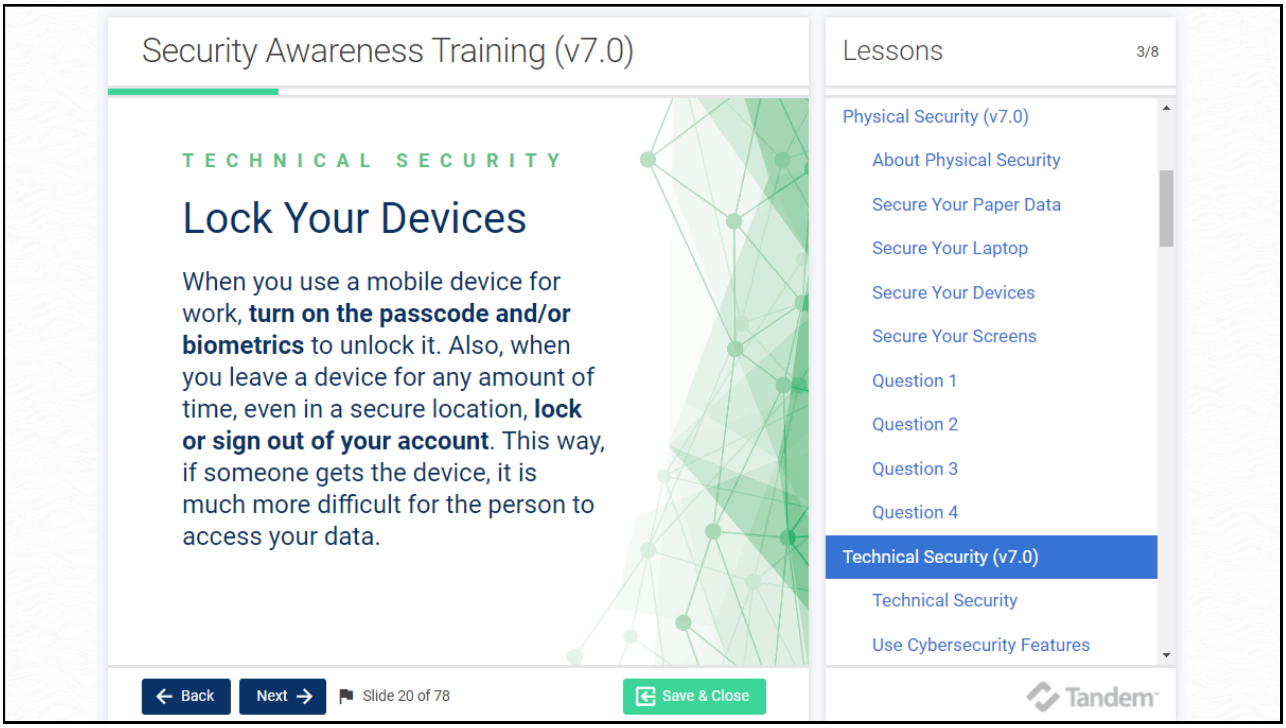
1 Train on what mobile devices employees can and can’t use.

2 Train on how to physically protect mobile devices.

3 Train on how to technically protect mobile devices.

Tandem

26



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

Slide 20 of 78

27

ADMINISTRATIVE CONTROLS: OFFBOARDING

1 Remove Access

2 Risk Assess

3 Reclaim Assets

Tandem

28

ADMINISTRATIVE CONTROLS: DOCUMENTS

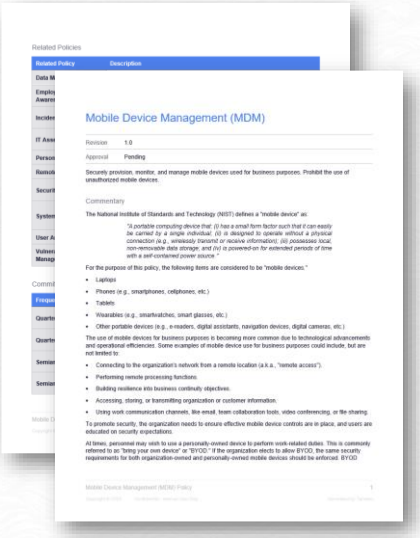
Mobile Device Management Policy

Acceptable Use Policy / Agreement

Nondisclosure Agreement (NDA)

Tandem

29



Related Policies

Related Policy	Description

Mobile Device Management (MDM)

Revision	1.0
Approval	Pending

Securely provision, monitor, and manage mobile devices used for business purposes. Prohibit the use of unauthorized mobile devices.

Commentary

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 connection (e.g., wirelessly 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."*

For the purpose of this policy, the following items are considered to be "mobile devices."

- 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.)

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:

- 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.

To promote security, the organization needs to ensure effective mobile device controls are in place, and users are educated on security expectations.

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

Mobile Device Management (MDM) Policy 1

Tandem.App/MDM-Policy-Template

SUBMIT YOUR QUESTIONS!

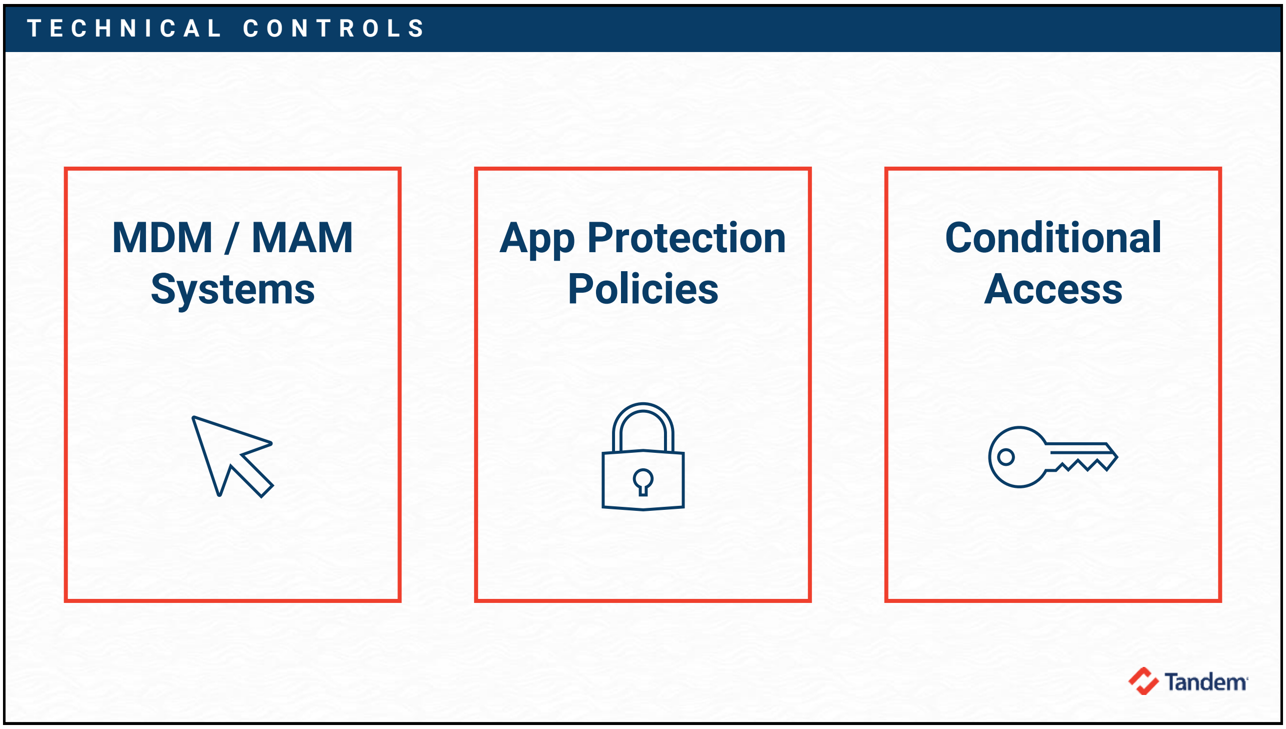
Tandem

30

MDM Technical Controls

Tandem

31

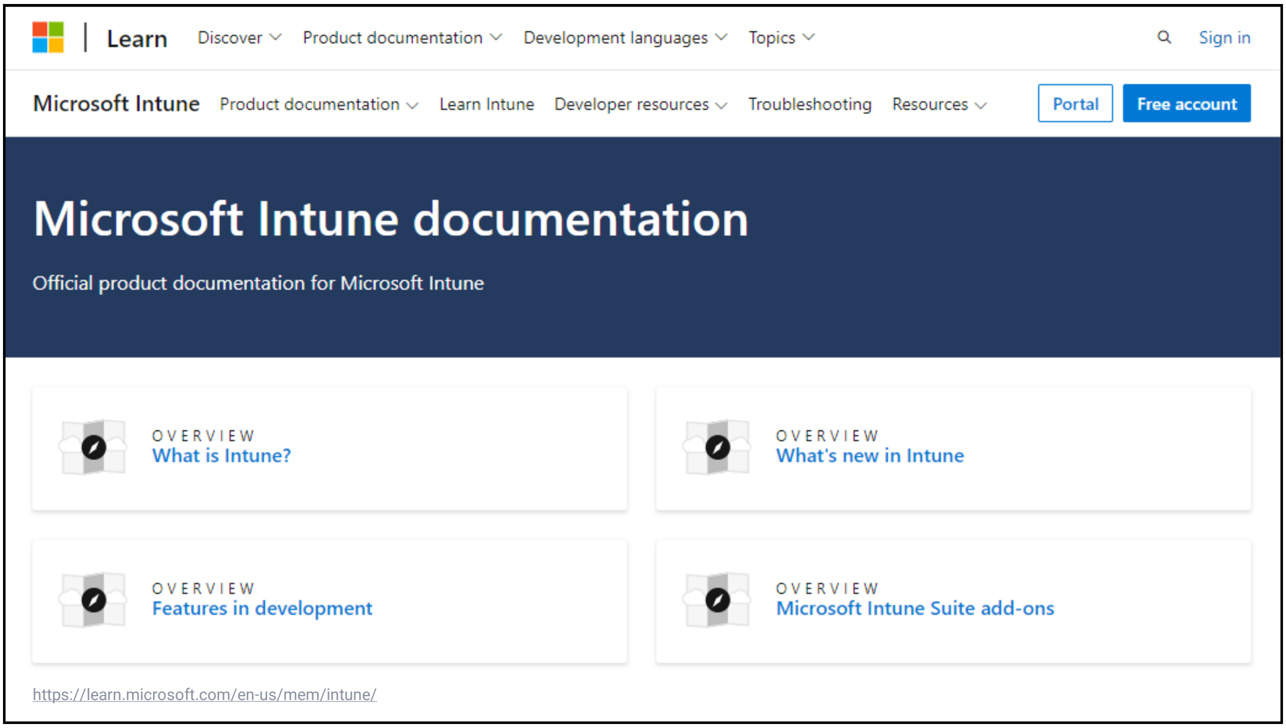


TECHNICAL CONTROLS

- MDM / MAM Systems
- App Protection Policies
- Conditional Access

Tandem

32



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

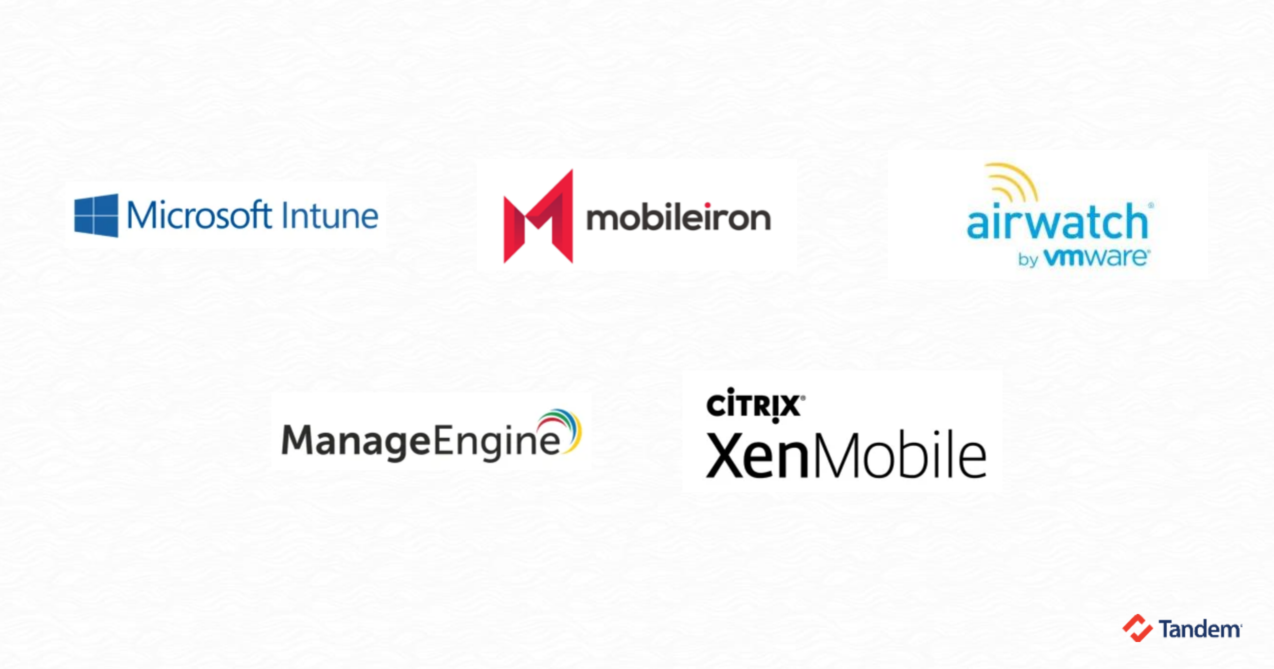
OVERVIEW
Features in development

OVERVIEW
Microsoft Intune Suite add-ons

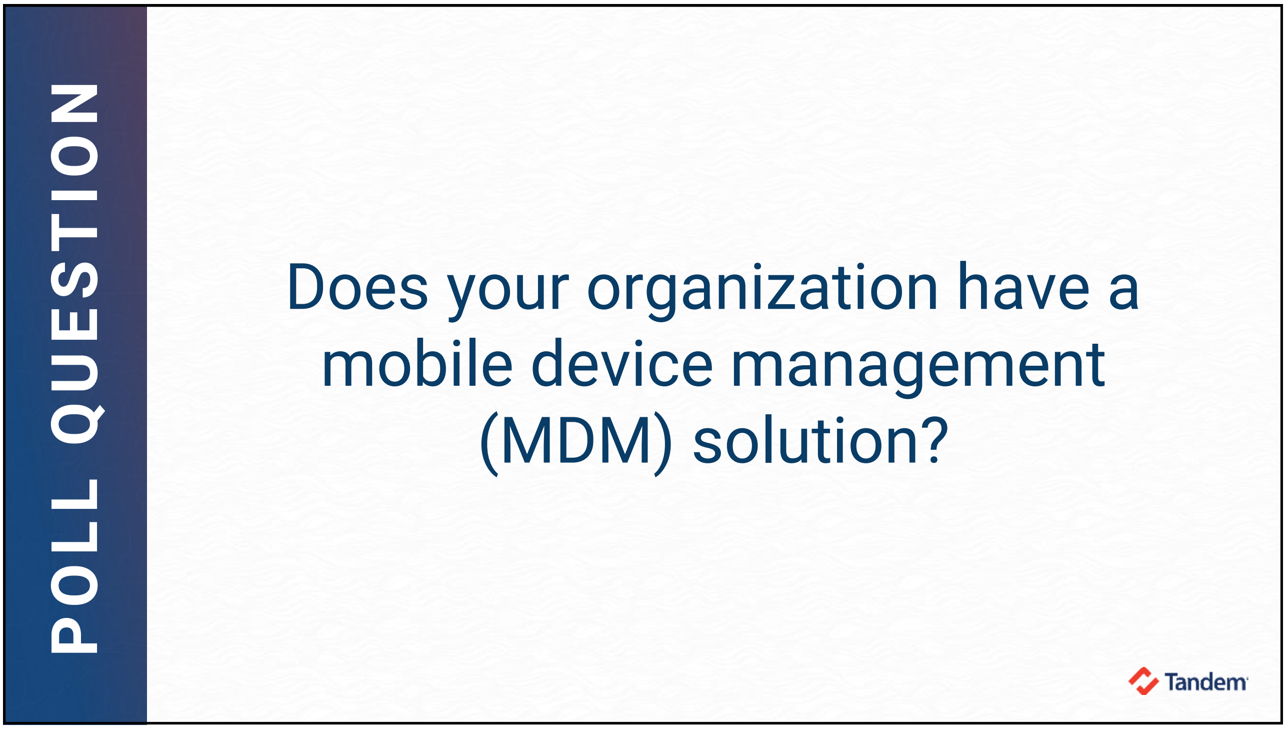
https://learn.microsoft.com/en-us/mem/intune/

33

MDM / MAM SYSTEMS



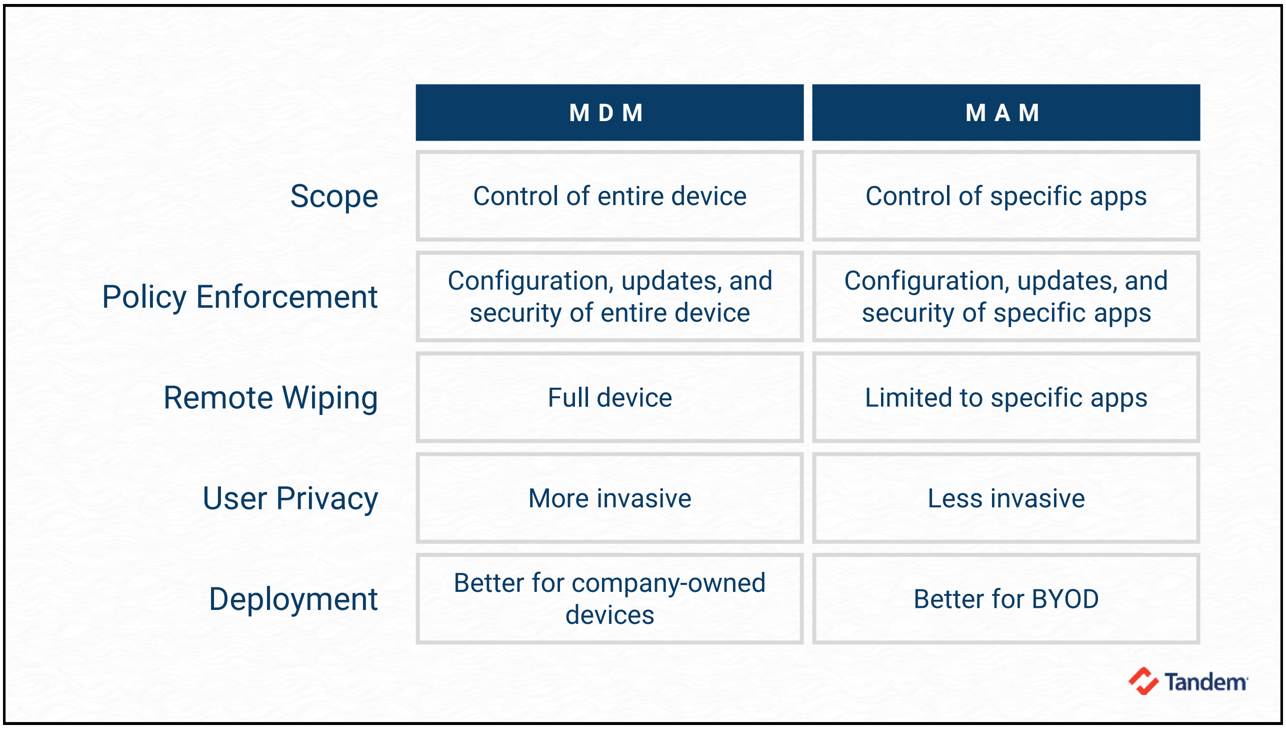
34



POLL QUESTION

Does your organization have a mobile device management (MDM) solution?

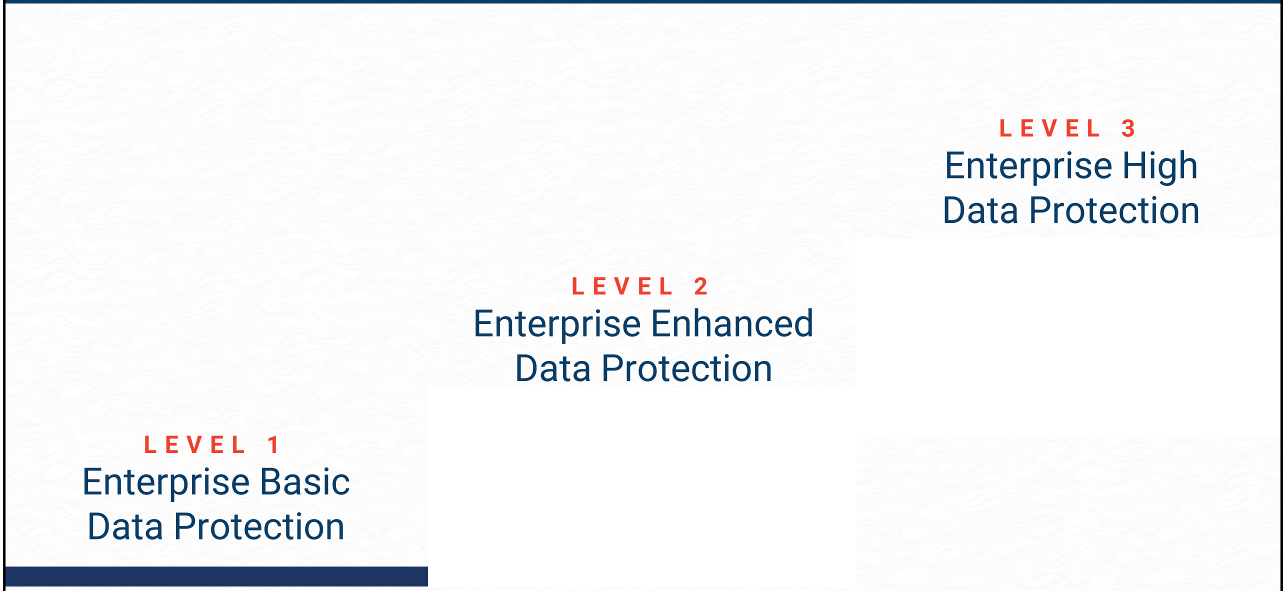
35



	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

36

APP PROTECTION POLICIES



LEVEL 3
Enterprise High Data Protection

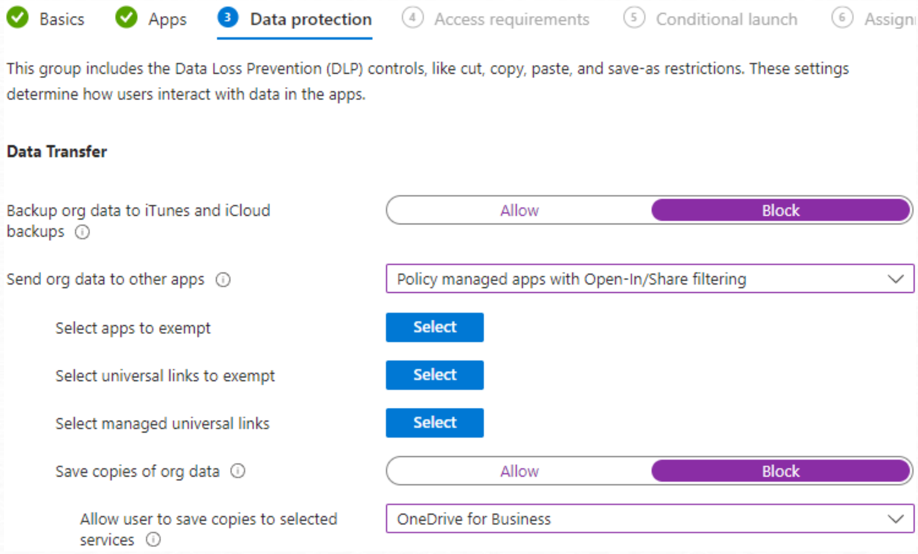
LEVEL 2
Enterprise Enhanced Data Protection

LEVEL 1
Enterprise Basic Data Protection

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

37

INTUNE EXAMPLE



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: Allow / [✓ Block]

Send org data to other apps: Policy managed apps with Open-In/Share filtering

Select apps to exempt: Select

Select universal links to exempt: Select

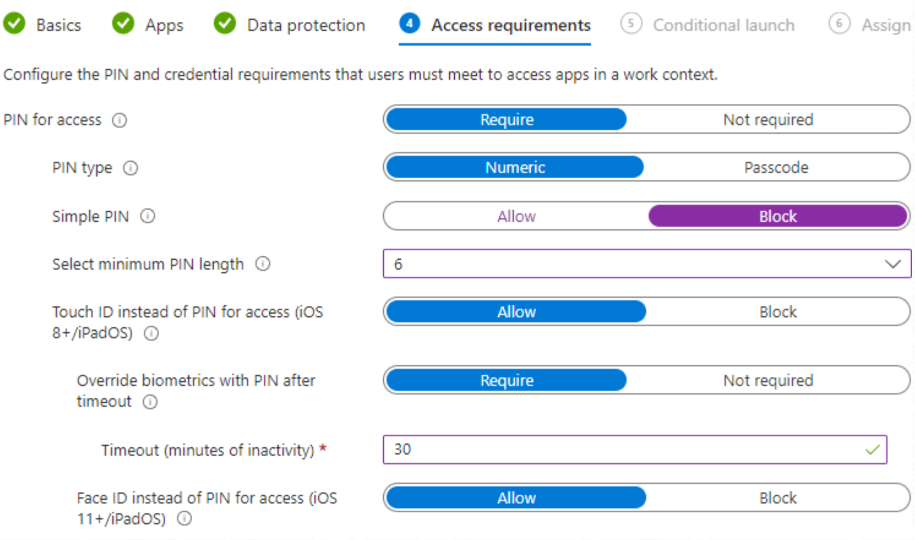
Select managed universal links: Select

Save copies of org data: Allow / [✓ Block]

Allow user to save copies to selected services: OneDrive for Business

38

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 ⓘ: [✓ Require] Not required

PIN type ⓘ: [✓ Numeric] Passcode

Simple PIN ⓘ: Allow [✓ Block]

Select minimum PIN length ⓘ: 6

Touch ID instead of PIN for access (iOS 8+/iPadOS) ⓘ: [✓ Allow] Block

Override biometrics with PIN after timeout ⓘ: [✓ Require] Not required

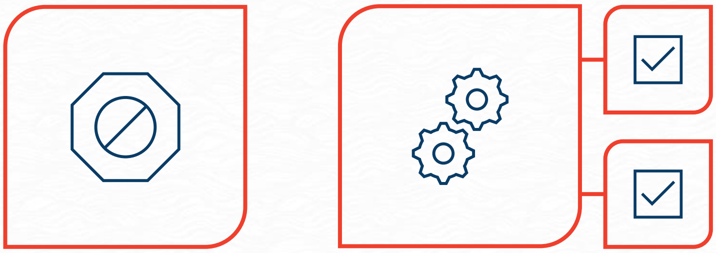
Timeout (minutes of inactivity) *: 30 ✓

Face ID instead of PIN for access (iOS 11+/iPadOS) ⓘ: [✓ Allow] Block

Tandem

39

EXAMPLE: CONDITIONAL ACCESS



Approved Client Apps

App Protection Policy

Block Exchange ActiveSync

Allow Access

* Applies to iOS and Android Devices
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

Tandem

40

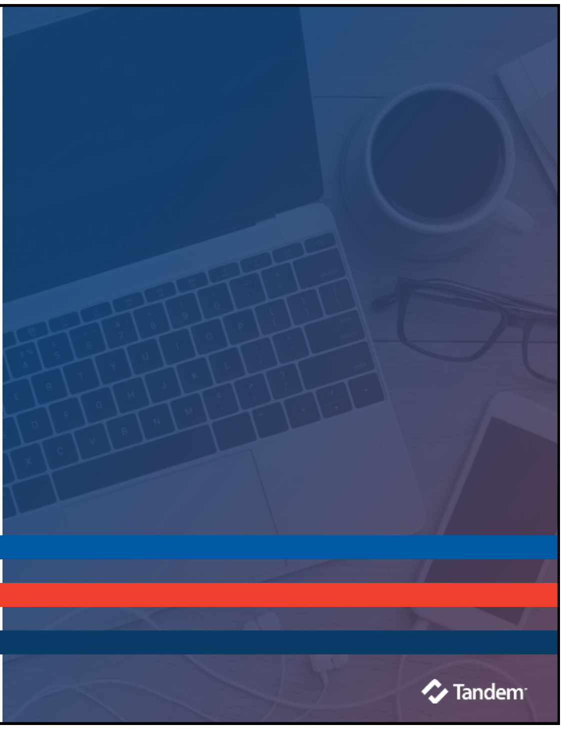
KEY TAKEAWAY

MDM tools help keep your data safe by making sure only the right people can access it at the right time.

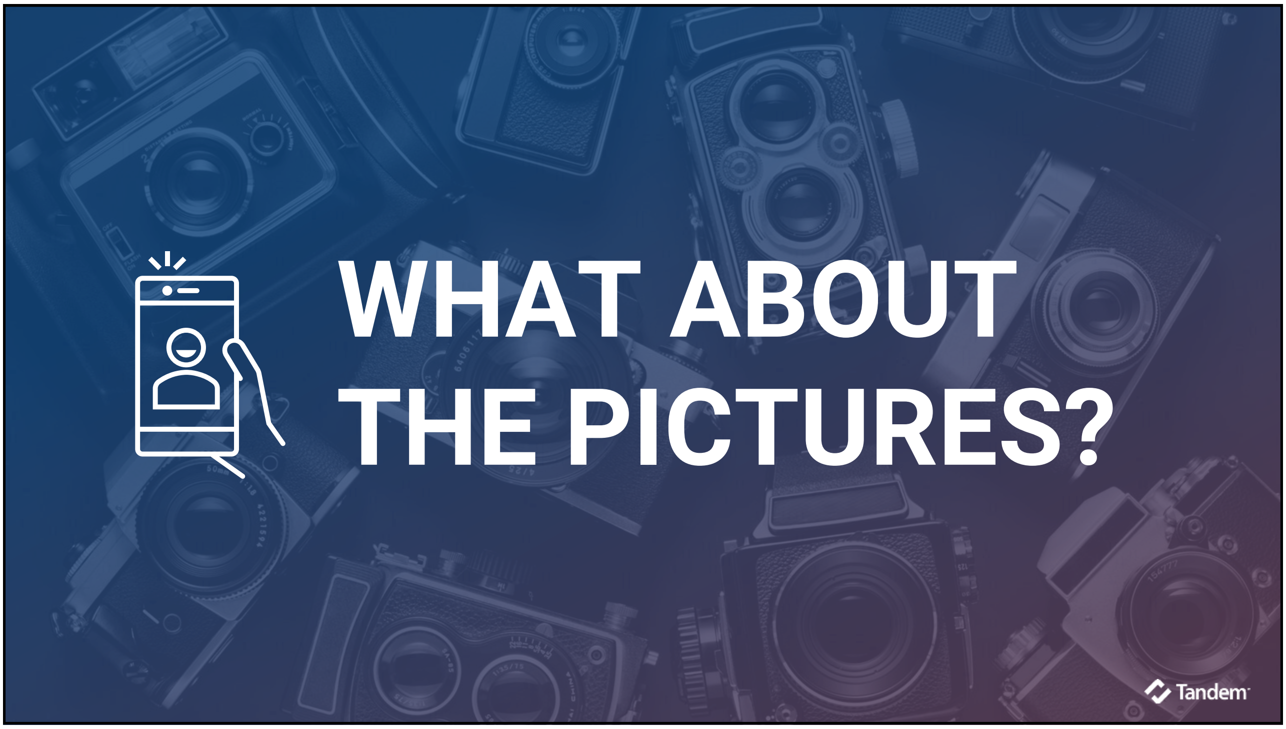
SUBMIT YOUR QUESTIONS!

41

Frequently Asked Question (FAQ)



42



WHAT ABOUT THE PICTURES?

43

Recap & Wrap Up

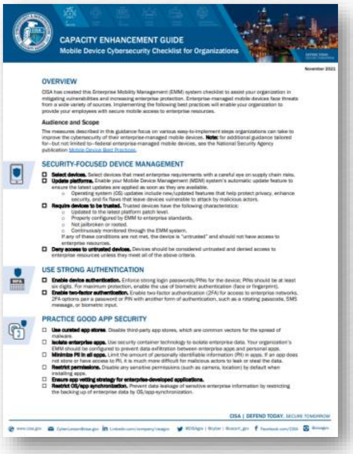
44

KEY TAKEAWAYS

1. Do mobile device management to protect your data.
2. Know 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.

Tandem

ADDITIONAL RESOURCES



CAPACITY ENHANCEMENT GUIDE

Mobile Device Cybersecurity Checklist for Organizations

November 2021

OVERVIEW

CISA has created this Enterprise Mobility Management (EMM) system checklist to assist your organization in mitigating vulnerabilities and increasing enterprise protection. Enterprise-managed mobile devices face threats from a wide variety of sources. Implementing the following best practices will enable your organization to provide your employees with secure mobile access to enterprise resources.

Audience and Scope

The measures described in this guidance focus on various easy-to-implement steps organizations can take to improve the cybersecurity of their enterprise-managed mobile devices. **Note:** for additional guidance tailored for—but not limited to—federal enterprise-managed mobile devices, see the National Security Agency publication Mobile Device Best Practices.

SECURITY-FOCUSED DEVICE MANAGEMENT

- □ **Select devices.** Select devices that meet enterprise requirements with a careful eye on supply chain risks.
- □ **Update platforms.** Enable your Mobile Device Management (MDM) system's automatic update feature to ensure the latest updates are applied as soon as they are available.
  - ○ Operating system (OS) updates include new/updated features that help protect privacy, enhance security, and fix flaws that leave devices vulnerable to attack by malicious actors.
- □ **Require devices to be trusted.** Trusted devices have the following characteristics:
  - ○ Updated to the latest platform patch level.
  - ○ Properly configured by EMM to enterprise standards.
  - ○ Not jailbroken or rooted.
  - ○ Continuously monitored through the EMM system.

  If any of these conditions are not met, the device is "untrusted" and should not have access to enterprise resources.
- □ **Deny access to untrusted devices.** Devices should be considered untrusted and denied access to enterprise resources unless they meet all of the above criteria.

USE STRONG AUTHENTICATION

- □ **Enable device authentication.** Enforce strong login passwords/PINs for the device; PINs should be at least six digits. For maximum protection, enable the use of biometric authentication (face or fingerprint).
- □ **Enable two-factor authentication.** Enable two-factor authentication (2FA) for access to enterprise networks. 2FA options pair a password or PIN with another form of authentication, such as a rotating passcode, SMS message, or biometric input.

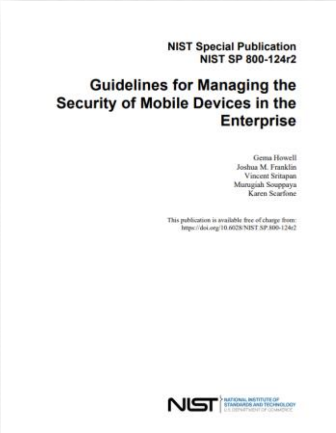
PRACTICE GOOD APP SECURITY

- □ **Use curated app stores.** Disable third-party app stores, which are common vectors for the spread of malware.
- □ **Isolate enterprise apps.** Use security container technology to isolate enterprise data. Your organization's EMM should be configured to prevent data exfiltration between enterprise apps and personal apps.
- □ **Minimize PII in all apps.** Limit the amount of personally identifiable information (PII) in apps. If an app does not store or have access to PII, it is much more difficult for malicious actors to leak or steal the data.
- □ **Restrict permissions.** Disable any sensitive permissions (such as camera, location) by default when installing apps.
- □ **Ensure app vetting strategy for enterprise-developed applications.**
- □ **Restrict OS/app synchronization.** Prevent data leakage of sensitive enterprise information by restricting the backing up of enterprise data by OS/app-synchronization.

CISA | DEFEND TODAY, SECURE TOMORROW

[illegible]

[CISA Mobile Device Cybersecurity Checklists]



NIST Special Publication
NIST SP 800-124r2

Guidelines for Managing the Security of Mobile Devices in the Enterprise

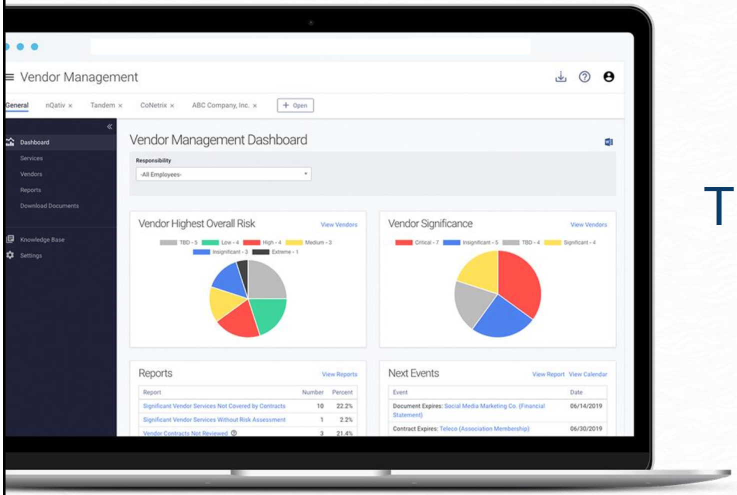
Gema Howell
Joshua M. Franklin
Vincent Sritapan
Murugiah Souppaya
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-124r2

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

[NIST SP800-124r2]

Tandem



Report	Number	Percent
Significant Vendor Services Not Covered by Contracts	10	22.2%
Significant Vendor Services Without Risk Assessment	1	2.2%
Vendor Contracts Not Reviewed	3	21.4%

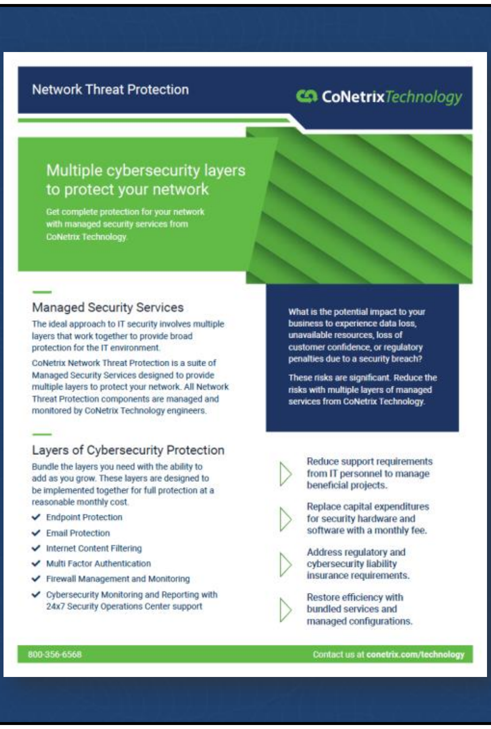
Event	Date
Document Expires: Social Media Marketing Co. (Financial Statement)	06/14/2019
Contract Expires: Teleco (Association Membership)	06/30/2019

LEARN MORE

Tandem Cybersecurity GRC Software

Tandem.App

47



Network Threat Protection

CoNetrix Technology

Multiple cybersecurity layers to protect your network

Get complete protection for your network with managed security services from CoNetrix Technology.

Managed Security Services

The ideal approach to IT security involves multiple layers that work together to provide broad protection for the IT environment.

CoNetrix Network Threat Protection is a suite of Managed Security Services designed to provide multiple layers to protect your network. All Network Threat Protection components are managed and monitored by CoNetrix Technology engineers.

What is the potential impact to your business to experience data loss, unavailable resources, loss of customer confidence, or regulatory penalties due to a security breach?

These risks are significant. Reduce the risks with multiple layers of managed services from CoNetrix Technology.

Layers of Cybersecurity Protection

Bundle the layers you need with the ability to add as you grow. These layers are designed to be implemented together for full protection at a reasonable monthly cost.

- ✓ Endpoint Protection
- ✓ Email Protection
- ✓ Internet Content Filtering
- ✓ Multi Factor Authentication
- ✓ Firewall Management and Monitoring
- ✓ Cybersecurity Monitoring and Reporting with 24x7 Security Operations Center support

- Reduce support requirements from IT personnel to manage beneficial projects.
- Replace capital expenditures for security hardware and software with a monthly fee.
- Address regulatory and cybersecurity liability insurance requirements.
- Restore efficiency with bundled services and managed configurations.

800-356-6568 Contact us at **conetrix.com/technology**

LEARN MORE

CoNetrix Technology Network Threat Protection

CoNetrix.com/Technology

Tandem

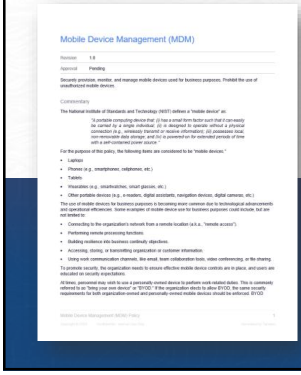
48

THANKS FOR JOINING

When Business is Personal: A Chat about MDM & BYOD

Chris Brewer, VCP
Team Lead
CoNetrix Technology, LLC
cbrewer@conetrix.com
LinkedIn.com/in/TheChrisBrewer

Alyssa Pugh, CISM, CRISC
GRC Content Manager
Tandem, LLC
apugh@tandem.app
LinkedIn.com/in/AlyssaPugh



Mobile Device Management (MDM)

Revision	1.0
Approval	Pending

Securely provision, monitor, and manage mobile devices used for business purposes. Prohibit the use of unauthorized mobile devices.

Commentary

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 connection (e.g., wirelessly 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."*

For the purpose of this policy, the following items are considered to be "mobile devices."

- 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.)

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:

- 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.

To promote security, the organization needs to ensure effective mobile device controls are in place, and users are educated on security expectations.

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

Mobile Device Management (MDM) Policy 1

Download the Template
Tandem.App/MDM-Policy-Template

☑ *Remember to complete the survey!*

Tandem

49