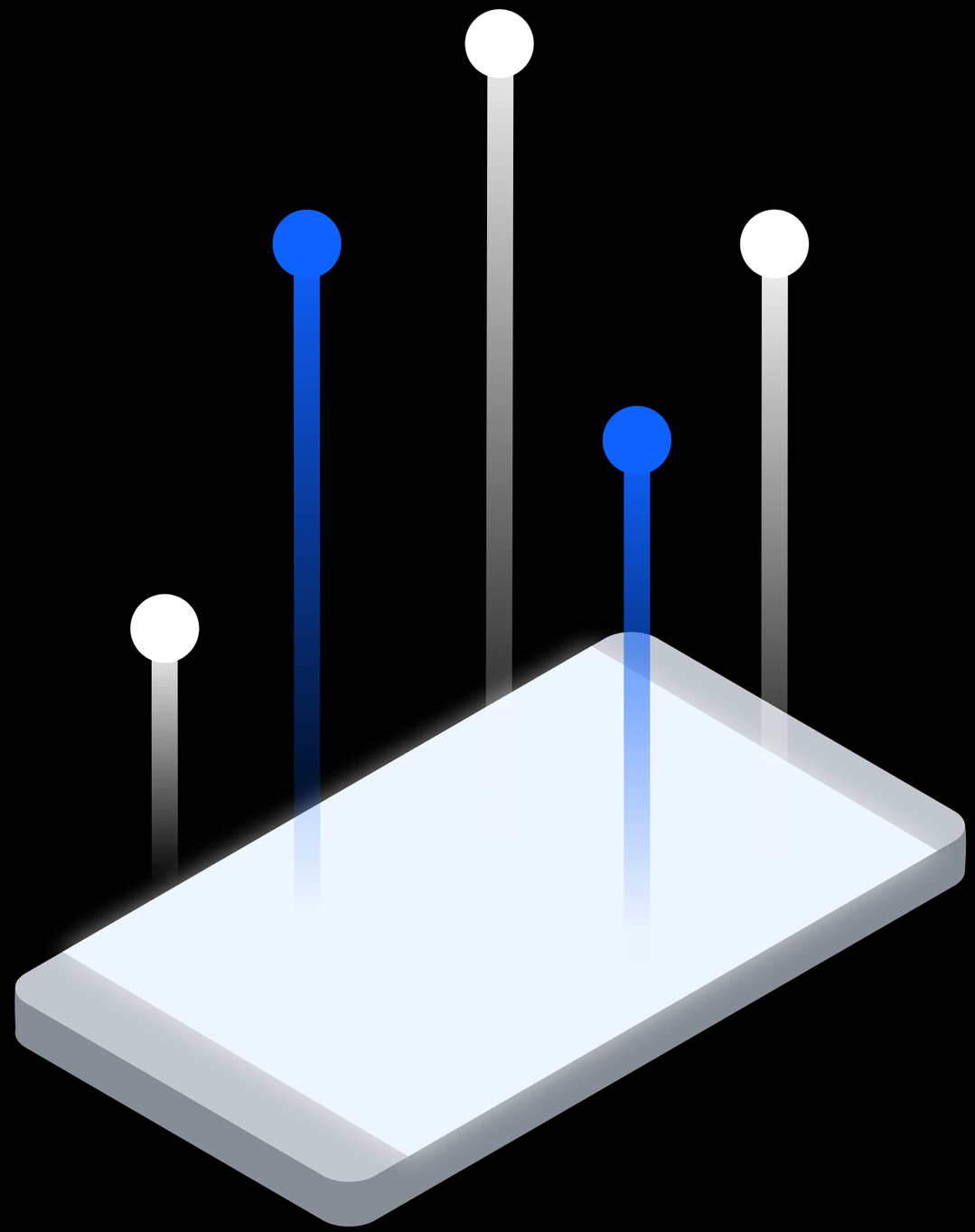
IBM **Security**

Top 10 Rules for BYOD

How to protect corporate data and privacy on personal devices used for work



IBM

How secure and productive is your BYOD program?

The rapid proliferation of mobile devices entering the workplace has come down like a lightning strike for many IT leaders. Mobile devices and their applications (apps) have transformed the way we live—how we communicate, travel, shop, work and so much more. This mobility transformation has been so revolutionary that it is hard to imagine life without these devices.

With BYOD, users can work any time at any place—and they'll be using the devices they paid for.

This raises the inevitable question: How will you support this demand while allowing users to be productive with email, apps and content in a safe environment that protects corporate data? Follow the "Ten rules for bring your own device" to create a peaceful, protected and productive mobile environment.

Ten rules for BYOD

1. Proactively create your policies
2. Find the devices that are accessing corporate resources
3. Make enrollment simple
4. Configure your devices over the air
5. Help your users help themselves
6. Protect the privacy of your users
7. Keep personal information separate from corporate
8. Manage data usage
9. Continually monitor devices for noncompliance
10. Measure the economic benefit from BYOD

Did you know...

Enterprise mobility management (EMM) expands upon mobile device management

(MDM) to offer app, content and expense management capabilities. Unified endpoint management (UEM) further supports additional types of devices, users and everything in between, including threat and identity management.

IBM

1

Proactively create your policies

Compliance, privacy, security, approved apps, and more need to be stated as clearly as possible in the acceptable usage agreement (AUA) or end user license agreement (EULA). It should be in plain enough language that everyone can understand as employees must also be required to sign one before they start using a device. If a device gets lost or stolen, emotions can run high so be sure to that procedures and actions are clear.

Historically, IT teams have had a firm grasp on hardware procurement and activation—e.g, tightly controlling how a device was configured, where and when it was used, and what software was installed—but in this BYOD age, policies must be documented and enforceable via a unified endpoint management (UEM) solution to give IT remote, automated authority as soon as an employee boots up a new phone, tablet or laptop.

Since there's no one right-sized BYOD policy, here are some questions to consider in developing your own:

- **Devices:** What device types will be supported? Smartphones, tablets, laptops, wearables? Only certain devices, or whatever the employee wants?
- **Compliance:** What regulations does your organization need to be in compliance with? The Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Financial Industry Regulatory Authority (FINRA) and the European Union's General Data Protection Regulation (GDPR) may be some to consider. Make sure you research the ones that are relevant to your industry or geography, and understand how they tie in to your mobile strategy.
- **Security:** What security measures are needed? Passcode and/or multi-factor authentication? Encryption? Containment? Jailbreak/root detection? Anti-malware? Conditional access? These are a few, but there are many to consider.
- **Apps:** Will you create a whitelist for approved apps? Or a blacklist for those that are prohibited? How will you deliver apps across the various devices in your environment (e.g. smartphones, tablets and laptops) while upholding a consistent user experience?
- **Agreements:** Is there an acceptable usage agreement (AUA) for employee devices accessing corporate data?
- **Corporate access:** What enterprise resources should your employees be able to access via mobile? Email, calendar and contacts? File shares and document repositories? Intranet sites? Wi-Fi networks? Virtual private networks?
- **User privacy:** You will need to protect the privacy of your users. What personal data is collected from employees' devices? What personal data is never collected? How will you communicate this to the organization?
- **Data plans:** Will the organization pay for the data plan? Will you issue a stipend, or will the employee submit expense reports?

No questions are off limits when it comes to BYOD. There must be frank and honest dialogue about how devices will be used and how IT can realistically meet expectations while protecting corporate data.

2

Find the devices that are accessing corporate resources

In the name of convenience, employees will connect multiple personal devices to corporate resources, but they may “forget” to tell you. The endpoint pool is getting deeper still with the advent of budget friendly Chrome OS and Windows 10 devices. To match this employee device sprawl, an organization should have tools that continuously monitor for existing accounts connecting from novel sources. Once a connection is detected, management can be applied to the device, or the account can be blocked outright.

To do this, you’ll need a tool that can communicate continuously with your email environment and detect all devices connected to your corporate network. Remember that once Microsoft ActiveSync is turned on for a mailbox, there are usually no barriers to syncing multiple devices without IT’s knowledge. All mobile devices need to be incorporated into your mobile initiative, and their owners need to be notified that new security policies are swinging into action.

Don’t know much about UEM?

UEM technology allows you to manage all device types on a single platform: laptops, desktops, smartphones, tablets, wearables and Internet of Things (IoT) devices.

3

Make enrollment simple

A satisfying user experience (UX) and clean user interface are now expectations, not luxuries. Without good UX or employee experience (EX), users will find easier workarounds to access resources, compromising productivity and security. Capabilities like Google Android Enterprise Zero-touch enrollment and the Apple Device Enrollment Program (DEP) make it dead simple. The user should be able to self-enroll, and IT teams should be able to bulk enroll devices based on business rules (like time-of-day and geographic location) and configurations (OS versions, available memory).

Any new devices trying to access corporate resources should be quarantined. This provides IT with the flexibility to block or initiate a proper enrollment workflow if approved, helping to ensure compliance with corporate policies. Think of your BYOD program as a prenuptial agreement that supports a harmonious union between users and IT policies. Simple yet detailed instructions should help users enroll in the BYOD program.

4

Configure your devices over-the-air

Over-the-air, or OTA, is one of those magical characteristics inherent to mobile technology-- and it's essential to keep employees from putting off updates because they can't get to the help desk or tether their device. Once enrollment is successful then OTA delivery of all all the profiles, credentials and settings the employee needs, including:

- Email, contacts and calendar
- VPN and Wi-Fi profiles
- Corporate content
- Internal and public apps
- Security policies (e.g., container)

See what they see

Finding a tool with built-in remote support capabilities can save additional time and effort down the road, when you need to conduct troubleshooting for users in the field.

5

Help your users help themselves

Most users prefer to try and fix issues themselves, but they'll stop once it gets too hard or time consuming and instead let it pile up in your help desk queue. A robust self-service platform will let your users directly:

- Initiate PIN and password resets
- Geo-locate a lost device with an interactive map
- Wipe a device remotely, and understand why they might be out of compliance.

How apptastic are you?

What's the best way to get apps down to devices? A universal app catalog makes it possible across all form factors and allows users to see which apps have been approved for use no matter which device they're on. You can track which users have installed them, and you can see which devices have the latest app version and who needs to install an update. The best app catalogs will look and feel just like public app stores—and even let users recommend and rate the ones they use.

6

Protect the privacy of your users

Personally identifiable information (PII) can be used to identify, contact, or locate a person. A growing number of international and local privacy laws prevent entities from collecting this data. Communicate the privacy policy to employees to make it clear what is and is not collected from their devices. To help, your UEM solution should be able to restrict the collection of:

- Personal emails, contacts, and calendars
- Location
- Photos
- App data and text messages
- Call history and voicemails
- Usernames and both hashed and unhashed passwords

An advanced solution keeps location and software information out of sight and out of mind. This helps companies meet PII regulations and provides added comfort for employees by preventing the viewing of PII on smartphones and tablets. For example:

- Disabling app inventory reporting to restrict administrators from seeing personal apps
- Deactivating location services to prevent access to location indicators such as physical address, geographical coordinates, IP address and Wi-Fi set service identifier (SSID)

7

Keep personal information separate from corporate data

Corporate apps, documents, and other data must be secured by IT if an employee separates from the organization, but personal email, apps, and photos should be untouched. This balance is achieved via an encrypted container—essentially a sandbox for corporate resources—available in most leading UEM solutions.

It's a win-win. Users appreciate the freedom of this approach while IT benefits from the ability to perform a selective wipe when an employee leaves the company, which includes email, calendar, contacts, apps and all corporate data—leaving personal data intact. Depending on the circumstances, if an employee loses the device, the option should also exist for the entire device to be wiped.

What makes a container great?

An on-device, passcode-protected container provides a home for all corporate data. The contained apps include corporate email, contacts, documents, chat and even a secure browser. You can provide users with their pertinent work resources all in one place. This is especially useful for contractors. It gives them all the resources they need, and lets you wipe it when their project is over and they leave. Don't need to manage the device, or only need to manage content? The best containers can be deployed standalone, eliminating the requirement of MDM device enrollment.

8

Manage data usage

Whether the data plan is being paid for by the employer or employee, you may want to help users track their current data usage and educate them about the benefits of using Wi-Fi when available AND within policy. You should be able to track in-network and roaming data usage on devices and generate alerts or outright block users once a specific data usage threshold is crossed.

You can set roaming and in-network megabit limits and customize the billing day to create notifications based on percentage used. Automatic Wi-Fi configuration helps ensure that devices automatically connect to Wi-Fi while in corporate locations.

9

Continually monitor enrolled devices for noncompliance

To keep auditors content and reduce vulnerabilities, you should configure device monitoring to detect certain conditions or violations and have automated remediation in place. Here are a few common user-generated issues that your policies should address:

“No mobile device management for me!” Users could try to remove corporate management from their device. Your policy should detect this and immediately restrict access to corporate resources.

“I’m breaking into this joint!” To bypass operating system (OS) limitations, employees sometimes jailbreak (Apple iOS) or root (Google Android) a device, opening the door to sideloading of apps, which in turn opens the door to malware that can steal information. If a device is jailbroken or rooted, the UEM solution should be able to take automated action, such as selectively wiping the container, corporate apps, and any sensitive data from the device right away.

“I can’t keep up with technology.” Restricting outdated OS versions helps ensure compliance and optimizes device operability. Your BYOD policy should stipulate OS version updates and your UEM solution should keep users up-to-date with the latest OS versions released by all major vendors, including Apple, Google, and Microsoft.

Go on a malware tear

Apps can be troublemakers. You have to know when malware is present on your devices, and respond right away so it doesn’t spread. Be selective with your EMM or UEM choice. It should give you a way to detect apps with malware signatures and malicious behavior so you can take action to stop them as soon as possible.

10

Measure the benefit from BYOD

If you follow the rules above, you will no doubt want to measure the economic and business benefits—in other words, the ROI of BYOD. Decreasing hardware costs is an obvious category, but you can go deeper. While the contrary is often assumed by many organizations new to BYOD, productivity often increases when employees become mobile and connected at all times and IT teams become more efficient.

As you're writing policy, consider how that policy will impact return on investment. That includes comparing approaches, as shown:

Corporate-owned model

- How much you would spend on each device
- The cost of a fully subsidized data plan
- The cost of recycling devices every few years
- Warranty plans
- IT time and labor in managing the program

BYOD

- The cost of a partially subsidized data plan
- The eliminated cost of the device purchase
- The cost of a mobile management platform

For an in-depth look at the potential ROI enterprises may realize by deploying a UEM solution supporting BYOD and remote work, read this **Forrester Total Economic Impact Study.**

Safely connect users to any resource

When UEM combines with identity and access management (IAM), it's a beautiful thing. It provides users with protected, single sign-on (SSO) and multi-factor access to the cloud and web apps needed for work. This reduces user irritation, because they do not have to remember multiple passwords for apps. They obtain the access they need without compromising data security.

BYOD is just the beginning

Enabling, securing and empowering remote workers has never been more urgent and a best-in-class BYOD deployment can be a cornerstone of your efforts to transforming your workplace and your workers.

To learn more about how IBM Security MaaS360 unified endpoint management can help you, please visit: **https://www.ibm.com/security/mobile/maas360**

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2020

00000000USEN