

FOR OPTIMAL VIEWING, PLEASE USE ACROBAT READER

Ten rules for bring your own device (BYOD)

How to protect corporate data on personal devices used for work

IBM Security
Thought Leadership White Paper



< Should you allow a BYOD workplace?

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.

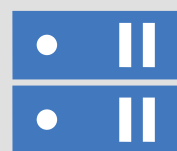
This raises the inevitable question: How will you support this demand while allowing users to be productive with email, apps and content in a safe environment that protects corporate data? Follow the “Ten rules for bring your own device” to create a peaceful, protected and productive mobile environment.

Ten rules for BYOD

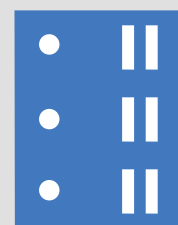
1. Create your policy before procuring technology
2. Find the devices that are accessing corporate resources
3. Make enrollment simple
4. Configure your devices over the air
5. Help your users help themselves
6. Protect the privacy of your users
7. Keep personal information separate from corporate data
8. Manage data usage
9. Continually monitor devices for noncompliance
10. Enjoy the return on investment from BYOD



EMM



MDM



UEM

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 endpoints, users and everything in between, including threat and identity management.

1

< Create your policy before procuring technology

Like any other IT project, policy must precede technology—yes, even in the cloud. To effectively use MDM or EMM technology for employee-owned devices, you still need to decide on policies. These policies affect more than just IT; they have implications for HR, legal and security—any part of the business that uses mobile devices, apps and content in the name of productivity.

Since all lines of business are affected by BYOD policy, it can't be created in an IT vacuum. With diverse users' needs, IT must make sure each individual is part of policy creation. 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 protection? 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 (VPNs)?
- **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

You likely have more devices accessing your network than you're willing to admit. Don't live in denial. What you don't know can hurt you. Understand the current landscape of your mobile device population before setting your strategy in stone.

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

Once you identify the devices you need to enroll, your BYOD program should use technology that allows for a simple and low-touch method for users to enroll—while allowing you to scale—limiting tedious, manual processes.

You want the ability to enroll devices in bulk—or for users to self-enroll their devices. You also need to authenticate employees with a basic authentication process such as a one-time passcode or use existing corporate directories such as Microsoft Active Directory/Lightweight Directory Access Protocol (AD/LDAP).

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.

These should be sent in an email or a text message that leads to an MDM profile being created on their device. Make sure to incorporate the ever-important AUA.

4



Configure your devices over the air

If there's one thing your BYOD policy shouldn't do, it's bring more users to the help desk. Your devices should be configured over the air (OTA) to save time and optimize efficiency for both IT and users.

Once users have completed their enrollment, your MDM or EMM platform should support OTA delivery of 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

Users want a functioning device, and you want to optimize help desk time. A robust self-service platform lets users directly:

- Initiate PIN and password resets in the event that they forget the current one
- Geo-locate a lost device from a web portal using mapping integration
- Wipe a device remotely to remove sensitive corporate data
- Understand why they may be out of compliance

Security, corporate data protection and compliance are shared responsibilities. It may be a hard pill for employees to swallow, but there is no chance of mitigating risk without their cooperation.



How *apptastic* are you?

You'll want to think of the best way to get apps down to devices. A universal app catalog makes it possible across all form factors. Taking this approach, users can 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

A well-crafted BYOD program will keep personal employee data off your screen. Personally identifiable information (PII) can be used to identify, contact or locate a person. Some privacy laws prevent corporations from collecting this data. Communicate the privacy policy to employees and make it clear what is and is not collected from their devices. For instance, an MDM or EMM 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

On the other hand, let users know what you collect, how it will be used, and why it benefits them.

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

Simply stated, corporate apps, documents and other materials must be protected by IT if the employee decides to leave the organization, but personal email, apps and photos should be untouched.

This balance is achieved with containment technology available from leading EMM solutions. Not only will users appreciate the freedom of this approach, but so will IT, whose life will likely be infinitely easier as a result. IT will be able to perform a selective wipe when an employee leaves the company, including email, calendar, contacts, apps and all corporate data. Depending on the circumstances, if an employee loses the device, the entire device can be wiped.



What makes a container great?

An on-device, passcode-protected container provides a home for all corporate data. The apps that live inside 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 goodies 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

If you pay for the data plan, you may want a way to track this data. If you are not paying, you may want to help users track their current data usage. You should be able to track in-network and roaming data usage on devices and generate alerts if a user crosses a threshold of data usage.

You can set roaming and in-network megabit limits and customize the billing day to create notifications based on percentage used. It's recommended that you educate users on the benefits of using Wi-Fi when available. Automatic Wi-Fi configuration helps ensure that devices automatically connect to Wi-Fi while in corporate locations.

If the stipend plan only covers USD50 or 200 MB of data usage a month, employees appreciate a warning that they're about to be responsible for overages.

9

Continually monitor devices for noncompliance

Once a device is enrolled, it's all about context. Devices should be continuously monitored for certain scenarios, and automated policies should be in place. Here are a few common issues that your policies should address:

"No MDM 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) restrictions, employees sometimes jailbreak (Apple iOS) or root (Google Android) a device, opening the door to malware that can steal information. If a device is jailbroken or rooted, the MDM or EMM solution should be able to take 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." Your BYOD policy should have a stipulation about OS version updates. You'll need to keep users up-to-date with the latest and greatest OS versions released by all major vendors, including Apple, Google and Microsoft. Restricting outdated OS versions helps ensure compliance and optimizes device operability.



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



Enjoy the return on investment from BYOD

One size doesn't fit all, but a carefully crafted BYOD policy can equip you with the direction you need to manage mobile devices effectively and efficiently.

Of course, productivity increases are often seen when employees are mobile and connected at all times. BYOD is a great way to bring this advance in productivity to new users who may not have been eligible for corporate devices previously. As you're writing policy, consider how that policy will impact return on investment. That includes comparing approaches, as shown below:

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



But wait...there's more!

When UEM combines with identity and access management (IAM), it's a beautiful thing. It provides users with protected, single sign-on (SSO) 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.





Net-net

BYOD has become a mainstay practice for all organizations, and it's no wonder why. It gives employees the freedom to work on their own devices while relieving significant financial and management burdens for IT and security leaders. However, BYOD cannot deliver on the promise of streamlined management and cost savings without a well-written policy and a robust management platform. If you're still in the early stages of your mobile strategy, IBM® MaaS360® with Watson™ offers a wealth of educational resources. If you've decided BYOD is right for your business, [click here](#) to experience a no-cost 30-day trial of MaaS360. Since MaaS360 is cloud-based, your test environment automatically becomes a production environment with no loss of data.



Moving forward, move beyond the basics

Managing endpoints plus their users and data is a time-consuming task with conventional MDM and EMM solutions. Cognitive UEM provides insights, contextual analytics and cloud-sourced benchmarking capabilities that help you make sense of the mobile minutiae you encounter daily—while protecting your endpoints, users, apps, docs and their data from one platform.

IBM MaaS360 | With Watson

About MaaS360 with Watson

Thousands of organizations of all sizes across all industries trust MaaS360 as the foundation for their digital transformation with mobile. With Watson, MaaS360 delivers cognitive UEM with strong security controls across users, devices, apps and content to support endpoint and mobile deployments. Delivered from a best-in-class IBM Cloud on a mature, trusted platform, MaaS360 helps to manage a wide variety of devices for multiple users from a single console, and to provide integration with solutions from Apple, Google, Microsoft and other suppliers of management tools. IBM works hand-in-hand with these suppliers not only to provide integration but also to ensure that integration can occur as soon as new tools or updates to existing tools are available.





For more information

For more information on MaaS360, and to start a no-cost 30-day trial, visit: ibm.com/maas360-trial

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 30 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: ibm.com/financing

© Copyright IBM Corporation 2018

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
January 2018

IBM, the IBM logo, ibm.com, MaaS360, Watson, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

Microsoft is a trademark of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.