IBM Security
Thought Leadership White Paper

Ten rules for Bring Your Own Device (BYOD)

Learn how to protect corporate data when users use personal devices for work

IBM

Should you allow BYOD?

The rapid proliferation of mobile devices entering the workplace appears to be like divine intervention to many IT leaders. Mobile devices and their apps have transformed the way we live – how we communicate, travel, shop, work and so much more. This mobility transformation has been so radical, so revolutionary, that it is hard to imagine life without these devices. Bring Your Own Device (BYOD) was born and employees followed with fervor.

There's no sense pretending it's not happening or saying, "We don't let our employees do that." The truth is, they're doing it already and will likely continue to burrow noncompliant devices into your network with or without your permission. By 2016, a majority of enterprise employees will be permitted to use their own smartphones and tablets for work purposes.

This raises the inevitable question: how will you support workforce desire to use personal apps and devices while allowing them to be productive in a safe environment that protects corporate data? *The ten rules for Bring Your Own Device (BYOD)* show you how to create a peaceful, protected, and productive mobile environment.

The ten rules for Bring Your Own Device (BYOD)

1. Create your policy before procuring technology
2. Find the devices that are accessing corporate resources
3. Enrollment should be simple
4. Configure your devices over-the-air
5. Help your users help themselves
6. Keep personal information private
7. Keep personal information separate from corporate data
8. Manage data usage
9. Continually monitor devices for noncompliance
10. Enjoy the return on investment (ROI) from BYOD

1. Create your policy before procuring technology

Like any other IT project, policy must precede technology – yes, even in the cloud. To effectively use mobile device management (MDM) 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 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 the diverse needs of users, IT must make sure they are all part of policy creation.

There's no one right BYOD policy, but here are some questions to consider:

- **Devices:** What mobile devices will be supported? Only certain devices or whatever the employee wants?
- **Data plans:** Will the organization pay for the data plan at all? Will you issue a stipend, or will the employee submit expense reports?
- **Compliance:** What regulations govern the data your organization needs to protect? For instance, the Health Insurance Portability and Accountability Act (HIPAA) requires native / encryption on any device that holds data subject to the act.
- **Security:** What security measures are needed (passcode protection, jailbroken/rooted devices, anti-malware apps, encryption, device restrictions, iCloud backup)?
- **Applications:** What apps are forbidden? IP scanning, data sharing, Dropbox?
- **Agreements:** Is there an Acceptable Usage Agreement (AUA) for employee devices with corporate data?
- **Services:** What kinds of resources can employees access – email? Certain wireless networks or VPNs? CRM?
- **Privacy:** What data is collected from employees' devices? What personal data is never collected?

No questions are off limits when it comes to BYOD. There must be frank and honest dialog about how devices will be used and how IT can realistically meet those needs.

2. Find the devices that are accessing corporate resources

Imagine this. You start using an MDM solution under the assumption your company is supporting 100 or so devices. You've kept a meticulous spreadsheet of device types and users – there shouldn't be any surprises. However, when you first go to view reporting, over 200 devices appear. This scenario is fact, not fiction. It occurs far more often than you would think.

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 the devices connected to your corporate network. Remember that once 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.

3. Enrollment should be simple

Complexity tends to breed non-compliance. Once you identify devices to enroll, your BYOD program should use technology that allows for a simple, low touch way for users to enroll. The process should be simple and protected, and configures the device at the same time.

In a perfect scenario, users should be able to follow an email link or text that leads to an MDM profile being created on their device – including accepting the ever-important AUA.

Think of BYOD as a marriage with the AUA as a prenuptial agreement that supports a harmonious union.

Instructions should help existing users enroll in the BYOD program. It's recommended that existing users clear their ActiveSync accounts so that you can isolate and manage corporate data on the device. New devices should start with a fresh profile.

From an IT perspective, you want the ability to enroll existing 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 Active Directory/LDAP. Any new devices trying to access corporate resources should be quarantined and IT notified. This provides IT with flexibility to block or initiate a proper enrollment workflow if approved, helping to ensure compliance with corporate policies.

4. Configure your devices over-the-air

If there's one thing your BYOD policy and MDM solution shouldn't do, it's bring more users to the help desk. Your devices should be configured over-the-air to optimize efficiency for both IT and business users alike.

Once users have accepted the AUA, your platform should deliver all the profiles, credentials, and settings the employee needs access to including:

- Email, contacts, and calendar
- VPN and Wi-Fi
- Corporate documents and content
- Internal and public apps

At this point, you'll also create policies to restrict access to certain applications and generate warnings when a user goes over their data usage or stipend limit for the month.

5. Help your users help themselves

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

- PIN and password resets in the event that the employee forgets the current one
- Geo-locate a lost device from a web portal, using mapping integration
- Wipe a device remotely, removing sensitive corporate data

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. A self-service portal can help employees understand why they may be out of compliance.

6. Keep personal information private

Of course, BYOD policy isn't just about protecting corporate data; a well-crafted BYOD program keeps personal employee data away from others, including IT. Personally Identifiable Information (PII) can be used to identify, contact, or locate a person. Some privacy laws prevent corporations from even viewing this data. Communicate the privacy policy to employees and make it clear what data you cannot collect from their mobile devices. For instance, an MDM solution should be able to parse what information it can access and what it cannot, such as:

- Personal emails, contacts, and calendars
- Application 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 MDM solution can turn privacy policy into a privacy setting to hide the location and software information on a device. This helps companies meet PII regulations and provides added comfort for employees by preventing the viewing of personal information on smartphones and tablets. For example:

- Disabling app inventory reporting to restrict administrators from seeing personal applications.
- Deactivating location services to prevent access to location indicators such as physical address, geographical coordinates, IP address, and Wi-Fi SSID.
- Transparency and clarity are important watchwords. There's much less resistance to BYOD policies when each person knows the rules.

7. Keep personal information separate from corporate data

For BYOD to be an agreement both IT and users can live with, personal information like birthday party photos or that great American novel should be isolated from productivity apps.

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 by corporate IT.

Not only will users appreciate the freedom of this approach, but so will IT, whose life will likely be infinitely easier as a result. With this approach, IT can selectively wipe corporate data when an employee leaves the company. Depending on the circumstances, if an employee loses the device, the entire device can be wiped. A true MDM solution can give you the choice.

It is estimated that some 86 percent of device wipes are selective; only corporate data is wiped.

8. Manage data usage

A BYOD policy largely takes IT out of the communications business, but many companies still need to help employees manage their data use in order to avoid excessive charges.

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 devices automatically connect to Wi-Fi while in corporate locations.

If the stipend plan only covers $50 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. Is the user trying to disable management? Does the device comply with security policy? Do you need to make adjustments based on the data you are seeing? From here, you can start understanding additional policies or rules to create. Here are a few common issues:

- **Getting to the "root" of jailbreaking:** To get paid apps for free, employees sometimes"jailbreak" or "root" a phone, opening the door to malware that can steal information. If a device is jailbroken, the MDM solution should be able to take action such as selectively wiping corporate data from the device right away.
- **Spare the wipe; send an SMS:** If time wasters like Angry Birds rub against corporate policies, but are not offenses, an automatic wipe is heavy handed. An MDM solution can enforce policies based on the offense. MDM can message the user, offering time to remove the application before IT hits the wipe button.
- **New operating system available.** For BYOD to remain effective, users need a simple way to be alerted when a new OS is ready for installation. With the right MDM solution, OS upgrades become a self-service function. Restricting out-of-date OS versions helps ensure compliance and optimizes device operability.

10. Enjoy the return on investment (ROI) from BYOD

While BYOD shifts responsibility for purchasing devices to employees, it's worth considering the big picture and long-term costs for your organization.

As you're writing policy, consider how that policy will impact ROI. 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

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.

BYOD: The security of freedom

BYOD is an emerging best practice for giving employees the freedom to work on their own devices while relieving IT's significant financial and management burdens. However, BYOD cannot deliver on these promises 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® 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 production with no loss of data.

About IBM MaaS360

IBM MaaS360 is the enterprise mobility management platform to enable productivity and data protection for the way people work. Thousands of organizations trust MaaS360 as the foundation for their mobility initiatives. MaaS360 delivers comprehensive management with strong security controls across users, devices, apps and content to support any mobile deployment. For more information on IBM MaaS360, and to start a no cost 30-day trial, visit www.ibm.com/maas360

About IBM Security

IBM's security platform provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development, and delivery organizations. For more information, please visit www.ibm.com/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
March 2016

Please Recycle

WGW03112-USEN-01