THE TEN COMMANDMENTS OF BYOD

MaaS360®
by Fiberlink, an IBM company

MaaS360® by Fiberlink, an IBM company

Thou Shalt Allow BYOD

The rapid proliferation of mobile devices entering the workplace feels like divine intervention to many IT leaders. It's as if a voice boomed down from the mountain ordering all of the employees you support to procure as many devices as possible and connect them to corporate services en masse. Bring Your Own Device (BYOD) was born and employees followed with fervor.

There's no sense pretending it isn't happening or saying, "We don't let our employees do that." The truth is, they're doing it already and will continue to burrow noncompliant devices into your network with or without your permission. Forrester's study of US information workers revealed that 37% are doing something with technology before formal permissions or policies are instituted. [1] Further, a Gartner CIO survey determined that 80% of employees will be eligible to use their own equipment with employee data on board by 2016. [2]

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 secure environment that protects corporate data? The Ten Commandments of BYOD show you how to create a peaceful, secure, and productive mobile environment.

The Ten Commandments of BYOD

1. Create Thy Policy Before Procuring Technology
2. Seek The Flocks' Devices
3. Enrollment Shall Be Simple
4. Thou Shalt Configure Devices Over the Air
5. Thy Users Demand Self-Service
6. Hold Sacred Personal Information
7. Part the Seas of Corporate and Personal Data
8. Monitor Thy Flock—Herd Automatically
9. Manage Thy Data Usage
10. Drink from the Fountain of ROI

[1] Benjamin Gray and Christian Kane, "Fifteen Mobile Policy Best Practices," Forrester Research, January 2011.

[2] Ken Dulaney and Paul DeBeasi, "Managing Employee-Owned Technology in the Enterprise," Gartner Group, October 2011.

MaaS360® by Fiberlink, an IBM company

1. Create Thy Policy Before Procuring Technology

Like any other IT project, policy must precede technology—yes, even in the cloud. To effectively leverage 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 ensure 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?

According to Forrester, 70% of smartphones belong to users, 12% are chosen from an approved list, and 16% are corporate-issued. Some 65% of tablets belong to users, 15% are chosen from a list, and 16% are corporate issued. In other words, users in most cases bring their own devices.

- **Data Plans:** Will the organization pay for the data plan at all? Will you issue a stipend, or will the employee submit expense reports?

Who pays for these devices? For smartphones, 70% paid the full price, 12% got a discount, 3% paid a partial amount, and in 15% of cases, the company covered the full price. With tablets, 58% bought their own, 17% got a corporate discount, 7% shared the cost, and 18% were issued and paid for by their companies. (Source: Forrester, 2011)

- **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.

MaaS360® by Fiberlink, an IBM company

2. Seek the Flock's Devices

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. But 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 engraving your strategy on stone tablets. To do this, you'll need a tool that can communicate in real time 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 Shall Be Simple

Nothing breeds noncompliance faster than complexity. Once you identify devices to enroll, your BYOD program should leverage technology that allows for a simple, low touch way for users to enroll. The process should be simple, secure, and configure 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 ensures a harmonious union.

Instructions should help existing users enroll in the BYOD program. We do recommend 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, ensuring compliance with corporate policies.

MaaS360® by Fiberlink, an IBM company

4. Thou Shalt Configure 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. All devices should be configured over-the air to maximize 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
- 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. Give Thy Users Self-Service

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 all 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.

MaaS360® by Fiberlink, an IBM company

6. Hold Sacred Personal Information

Of course, BYOD policy isn't just about protecting corporate data; a well-crafted BYOD program holds employee data sacred and secure. 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 WiFi SSID

Transparency and clarity are important watchwords. There's much less resistance to BYOD policies when everyone knows the rules.

7. Part the Seas of Corporate and Personal Data

For BYOD to be an agreement both IT and end 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 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. But only a true MDM solution can give you the choice.

Some 86% of device wipes are selective; only corporate data is wiped.

MaaS360® by Fiberlink, an IBM company

8. Monitor Thy Flock—Herd Automatically

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 any 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 immediately.
- **Spare the Wipe; Send an SMS:** If time wasters like Angry Birds rub against corporate policies but are not offenses, an immediate 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 ensures compliance and maximizes device operability.

9. Manage Thy Data Usage

A BYOD policy largely takes IT out of the communications business, but most 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. We also recommend educating users on the benefits of using WiFi when available. Automatic WiFi configuration helps ensure devices automatically connect to WiFi 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.

MaaS360® by Fiberlink, an IBM company

10. Drink from the Fountain of ROI

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 in the following table:

Corporate-owned model	BYOD
How much you'd spend on each device	The cost of a partially subsidized data plan
The cost of a fully subsidized data plan	The eliminated cost of the device purchase
The cost of recycling devices every few years	The cost of a mobile management platform
Warranty plans	
IT time and labor in managing the program	

One size never fits all, but a carefully crafted BYOD policy arms 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 affording employees the freedom to work on their own devices while relieving IT of significant financial and management burdens, but BYOD will never deliver on these promises of streamlined management and cost savings without a well-written policy and a robust management platform.

If you've decided BYOD is right for your business, click here to start using MaaS360 for thirty days free. Since MaaS360 is cloud-based, your test environment immediately becomes production with no loss of data.

If you're still in the early stages of your mobile strategy, MaaS360 offers a wealth of educational resources including the following:

www.maas360.com
http://www.maas360.com/products/mobile-device-management/
MaaSters Center

For More Information
To learn more about our technology and services visit www.maaS360.com.
1787 Sentry Parkway West, Building 18, Suite 200 | Blue Bell, PA 19422
Phone 215.664.1600 | Fax 215.664.1601 | sales@fiberlink.com