



Breaking BlackBerry

10 Steps to Mobile Recovery & Continuity



Copyright © 2013 Fiberlink Communications Corporation. All rights reserved.

This document contains proprietary and confidential information of Fiberlink. No part of this document may be used, disclosed, distributed, transmitted, stored in any retrieval system, copied or reproduced in any way or form, including but not limited to photocopy, photographic, magnetic, electronic or other record, without the prior written permission of Fiberlink.

This document is provided for informational purposes only and the information herein is subject to change without notice. Please report any errors to Fiberlink. Fiberlink will not provide any warranties covering this information and specifically disclaims any liability in connection with this document.

Fiberlink, MaaS360, associated logos, and the names of the products and services of Fiberlink are trademarks or service marks of Fiberlink and may be registered in certain jurisdictions. All other names, marks, brands, logos, and symbols may be trademarks or registered trademarks or service marks of their respective owners. Use of any or all of the above is subject to the specific terms and conditions of the Agreement.

Copyright © 2013 Fiberlink, 1787 Sentry Parkway West, Building Eighteen, Suite 200, Blue Bell, PA 19422.

All rights reserved.



Breaking BlackBerry 10 Steps to Mobile Recovery & Continuity

Table of Contents

BlackBerry Death Knell?	5
Plan for Success	5
Step 1: Formalize Your Mobility Transition Initiative	6
Step 2: Develop Mobile Program Terms and Conditions	7
Step 3: Assess IT Environment Impact and Device Suitability.....	8
Step 4: Prepare and Inform the User Community	9
Configure and Test Your Solution	10
Step 5: Set Up Your Environment.....	10
Step 6: Launch a User Pilot Group	10
Deploy to End Users	11
Step 7: Enable Support Desk Teams.....	11
Step 8: Track and Report on Deployment Status	11
Step 9: Track Issues	11
Step 10: Ongoing Policy and Program Review	12
Conclusion	12
About MaaS360	13
Appendix A: BYOD Policy Guide	14
Introduction	14
Eligibility	14



Employee awareness of risks and responsibilities	15
End-user support	15
Policy violations	15
Device security and controls	15
Appendix B: Personal Device Usage Policies and Guidelines (Sample).....	17
Overview.....	17
Purpose.....	17
Definitions.....	17
Scope	17
Eligibility	18
References	18
Responsibilities	20
Procedures and Security	20
Expectation of Privacy.....	20
User Acknowledgment And Agreement	21
Appendix C: BYOD Policy FAQs (Sample).....	22



“IT and business leaders are looking for alternatives; an August 2013 Gartner survey showed only 9% of users at organizations expect to be on BlackBerry by 2016, compared to 24% today.”

– Ken Dulaney, Gartner

BlackBerry Death Knell?

With just one financial report and one analyst quote, the entire mobility industry has changed. BlackBerry, once the king of mobility, has quickly been relegated to court jester...or completely banished from the kingdom. While companies have been implementing bring your own device (BYOD) and corporate-owned, personally-enabled (COPE) programs for several years, very few considered the unthinkable: What would we do if BlackBerry were no longer available? Now, not only are enterprise IT departments asking the question, they are scrambling for answers.

According to a recent Gartner report, BlackBerry had nearly \$1 billion in unsold smartphones, may become a private company through acquisition, and recently laid off 40% of its global workforce. Gartner strongly recommends that enterprises still reliant on BlackBerry take action now.

It's time to look ahead and develop a plan to proactively phase out BlackBerry from your enterprise mobility program.

Until now, full BlackBerry replacement has not been a primary goal in most BYOD/COPE initiatives. The prevailing expectation was that BlackBerry would phase itself out organically and there was no need for proactive withdrawal. New realities require new thinking, and while the goal may not be immediate replacement, it is now imperative to develop and implement a plan to remove BlackBerry devices from the mobility management toolbox. Gartner recommends that you revisit your relationship with BlackBerry and update your strategy every three months.*

That's the bad news. Now, the good news.

All the progress you've made to support the use of employee- and corporate-owned iOS, Android and Windows Phone devices is going to pay off. If you have an informal, unstructured BYOD/COPE project in the early phases of adoption and deployment, you can easily add contingency plans for a possible BlackBerry shutdown. Even if BlackBerry does survive, your mobility management program will be more nimble and will be able to handle future market shifts.

Read on to learn how your successful BYOD/COPE program can incorporate BlackBerry shutdown readiness. If you have already tackled some of these steps, you are well on your way to a future-proof program, but don't rest on your laurels—swift action is not only warranted, it's essential.

Plan for Success

Setting a goal to wean the organization from BlackBerry use is a good idea. Developing a plan will ensure you can actually meet that goal successfully and within a defined time period.

Ken Dulaney, *“BlackBerry Announcements Require Enterprises to Take Action,”* Gartner, September 27, 2013.



Step 1: Formalize Your Mobility Transition Initiative



While mobile started as an organic endeavor, those days are long behind us. Like any other IT project, a formal initiative, complete with senior executive sponsorship and support, will ensure that your mobility transition project can proceed smoothly and effectively.

Assemble the Team and Initiate the Project

Create an implementation project plan and set milestones. Identify resources, roles and responsibilities, and assemble a cross-functional team with a common set of goals. Have frequent meetings and communicate goals, progress, and status to executive sponsors regularly.

Determine Your Organization's Policy Goals and Risk Tolerance

Moving from BlackBerry devices to iOS, Android and Windows Phone devices will involve reconsidering your organization's overall risk tolerance and how it views the application of security controls.

The BlackBerry platform provided virtually everything needed to secure company data on BlackBerry devices when properly implemented. With a proliferation of devices and operating systems, it is critical to document organizational goals for data and device security. Typical policy goals include:

- Protect intellectual property, customer and employee data, and the company's reputation by preventing the intentional and unintentional compromise of data through the use of personal and corporate mobile devices.
- Extend corporate security and acceptable use guidelines, procedures and regulatory mandates to mobile deployment.
- Respect and protect mobile device users' privacy and personal data, to the extent it can be protected given corporate security and regulatory guidelines.

These policy goals will be critical in the next steps.

***"A goal without
a plan is just a
wish."***

**– Antoine de Saint-
Exupery**



Step 2: Develop Mobile Program Terms and Conditions



End User Terms and Conditions

Draft a set of general policies to meet the organizational and departmental security goals and requirements.

Using these policies, create a set of documents that includes Mobile Device Policies, Usage Guidelines and a User Acceptance Agreement. These documents should clearly describe responsibilities, guidelines, and terms of use for company and employee-owned mobile devices that are configured for corporate use.

Using the documents as a guide, develop detailed mobile device and application policies and compliance rules/actions to implement and enforce them. These detailed policies and rules will be critical when configuring tools and certifying devices.

Fiberlink, the makers of MaaS360, have developed this free guide to help you draft your BYOD policies and take into account key considerations for your program.

BYOD/COPE Usage Terms and Restrictions

Document additional usage terms specifically for BYOD, and include the mobile policies, device types and services supported.

Take advantage of this free template to customize your own personal device usage policies and guidelines for your BYOD program.

Personal Privacy and Data Protection

Determine what personal information will be collected from devices and how personal data will be treated when a device is lost or stolen, or employment ends. Document, publish and communicate this policy, and make it part of the User Acceptance Agreement.



Step 3: Assess Alternative Solutions, IT Environment Impact and Device Suitability



Enterprise Mobility Management (EMM) Platform Evaluation

Evaluate leading EMM platforms, including MaaS360 by Fiberlink, to manage and secure mobile devices, applications, documents, email and Web access. Understand the features, multi-platform device support and configuration options that best meet your security, privacy and organizational goals.

Consider the available deployment options as you transition from your on-premises-only BES platform. Depending on your security, regulatory, budgetary and resource needs, you can look ahead and determine whether to transition to a cloud solution or remain with an on-premises offering.

Data Containment Solution Review

As you plan your transition from BlackBerry's secure and closed system, determine whether you will continue to need strong data containment solutions that separate corporate from personal data with a dual persona approach, or consider a shift to light security that maintains the native user experience of modern mobile devices. Understand your tolerance for corporate data leakage to balance your need for tight security with user satisfaction.

Mobile Application Management and Security Assessment

Compared with the expansive mobile app ecosystems of the iOS and Android platforms, BlackBerry's is still in its infancy. Even BlackBerry admitted in a recent regulatory filing that not having enough desirable apps is contributing to their decline. Consider deploying customized enterprise app catalogs to your users with mobile apps that are critical to your organization to increase employee productivity. Review app security features such as app wrapping or app software development kit (SDK) to require authentication, enable data leak prevention, perform compliance checks, and take enforcement actions. Assess your requirements for blacklisting, whitelisting or requiring apps.

Enterprise Architecture Impact

Document how these new systems required to support the BYOD/COPE deployment (Mobile Device, Application and Content Management, etc.) will fit into the enterprise architecture and the various integration points (Exchange, Active Directory, LDAP, BES, Certificates). Understand



the various roles, groups, policies and access rights that will be used when policies and rules are applied. Include any areas of impact that need to be considered.

Mobile Device Certification Process and Criteria

Develop and communicate a set of device criteria and a process for device certification. Device certification criteria should be based on stated policy goals and should have specific security control requirements to meet those goals. Pay special attention to the gaps between what BlackBerry is currently providing and what can be accomplished on the iOS, Android and Windows Phone platforms. Effectively communicating your device certification criteria and process can head off issues when devices that do not meet security goals come into the environment.

Step 4: Prepare and Inform the User Community



Communication Plans

Build plans and disseminate communications early and often to inform employees of the various policies, guidelines and user agreements. Provide a mechanism to collect feedback and comments, even if it's a blog or even a simple email box.

Enterprise Mobility Management Training Materials

Develop end-user training materials that provide guidance on the enrollment process and self-service portal functions. Use this free template to customize a set of FAQs (Frequently Asked Questions) for your BYOD policies to distribute to users.

Provide these documents in an easily-accessible location in mobile and non-mobile formats.



Configure and Test Your Solution

Step 5: Set Up Your Environment



Enterprise Integration

Initiate the configuration and integration of mobile device management systems with the larger enterprise infrastructure and the various integration points, including Exchange, Active Directory, LDAP, BES, and Certificates Authorities. Implement the various roles, groups, policies, and access rights for your organization and users.

Mobile Device Enrollment and Profiles

Create configuration profiles to support certificates, proxies, VPN, Wi-Fi, and enable the EMM system to support self-service device enrollment and rollout.

Mobile Device Policy and Compliance

Create device, application, content and user security policies in your selected EMM platform to meet mobile policy goals and intent. Use compliance rules to monitor and enforce policy compliance and as a communication tool to help users understand their obligations to protect corporate resources. Configure EMM privacy settings to align with the User Acceptance Agreement and intent of the program.

Step 6: Launch a User Pilot Group



Build confidence and refine plans by deploying to a small set of pilot users. Gather and document feedback from these users and adjust the platform, policies and configuration based on it.



Deploy to End Users

Step 7: Enable Support Desk Teams



Provide training and support for the front line Service Desk.

Leverage escalation processes to involve the appropriate subject matter experts from within the organization and from vendors.

Step 8: Track and Report on Deployment Status



Track and report on the status of the implementation including the number of devices enrolled, types and frequency of issues, and user feedback.

Step 9: Track Issues



Fully integrate into incident management systems and track issues to resolution ensuring escalation to the appropriate resource (internal or external). Require all stakeholders to attend incident review sessions.

Implement a feedback mechanism and ensure that changes and improvements are executed to support the project.



Step 10: Ongoing Policy and Program Review



Remember that you are building a program on a shifting foundation. The mobility market—its devices, operating systems, applications and capabilities—are changing almost daily. Revisit your policies and processes at least quarterly to ensure that new technologies are appropriately incorporated and user needs are accommodated. While the future of BlackBerry is certainly bleak, a program that is flexible enough to account for new entries and sudden exits in the marketplace can ensure that your organization's data is secure on any platform.

Conclusion

With a robust BYOD/COPE program, you will be able to quickly transition BlackBerry users to alternate devices. If BlackBerry should suddenly go dark, many users will already have access to a non-BlackBerry device that they can quickly enroll to get access to corporate data without compromising security. You may even choose to be proactive and remove BlackBerry from your environment altogether to avoid outages and/or degradation in service. A well-structured and functioning BYOD/COPE program will have many benefits to your organization beyond providing a much-needed BlackBerry contingency option.



About MaaS360

MaaS360 by Fiberlink is an enterprise mobility platform that enables IT to deliver end-to-end security and management for devices, applications, documents, email and Web access. Businesses, government agencies and educational institutions use MaaS360 to provide secure access to resources and content from mobile devices, without compromising the user experience, data security or privacy.

MaaS360 delivers maximum flexibility for bring your own device (BYOD) with a dual persona approach, multi-platform support, self-service enrollment, customized over-the-air configuration, automated policy enforcement, and secure distribution of apps and documents.





Appendix A: BYOD Policy Guide

Introduction

The following guide provides information and guidance on the areas that the End User Agreement and the Policies and Guidelines documents should address.

NOTE: *If you require assistance in the formulation and implementation of End User Agreements and Policies and Guidelines, the **Fiberlink Mobile Advisory Practice** is available to compliment your efforts and can provide your organization with an experienced consultant to help make your mobile project a success.*

Eligibility

Policy and guidance should address the following eligibility topics:

- Employee eligibility criteria including roles, titles and whether management approval is required and the process for approvals
- Geographic and organizational eligibility
- Eligibility based on device ownership and the difference in the services and applications available based on the above criteria
- Types of devices that are eligible for employee-liable device access

Employee awareness of risks and responsibilities

Employee awareness is an element of policy guidance and should include the following topics:

- The process and timeframe for reporting a lost or stolen device, and the situations for handling the decommissioning of a device if replaced or upgraded
- The process when a user is no longer eligible for access or leaves the company
- Specific identification of risks related to potential wiping of a user's entire device or just the corporate data, and the effects that will have on the user's data
- Self-service portals and tools to help the user locate or wipe their device
- Device passcode requirements (strength, history, expiration)
- Device restrictions that will be applied such as restricting camera, Bluetooth, or other applications and services
- Specifics related to compliance with stated policies including device jailbreaking or rooting, and unauthorized OS upgrades
- User responsibilities to backup personal data and applications



- Policy on sharing the device with family, friends and co-workers
- Inform the user that in the course of managing and securing the corporate data on their device, that certain information will be visible to IT including location, personal applications and data usage statistics (MaaS360 has BYOD privacy settings that can disable the collection of location information and personal app inventory.)
- Reminders and pointers to generic acceptable-use guidelines related to public and corporate network access and their obligations to adhere to all guidance when using mobile devices and applications
- Warnings that business use of a personal device may increase data plan usage and the responsibilities associated with overages and monitoring of usage

End-user support

The user will need to know, in detail, how to get support and how responsibilities are divided:

- How to apply and get approval to participate in the mobile device program
- How to enable a device
- Access to any related self-service portals and instructions on how to use them
- Links to all of the Acceptable Use and End User Agreements
- Details about the level of support that users will receive, and the differences between the corporate-liable and employee-liable device support, with a listing of the applications, services and scenarios that will be supported
- For employee-liable devices, indicate the user's responsibility to interact with the carrier/vendor of the device for support of services and applications that are not provided by the company

Policy violations

Provide clear language on the consequences of not adhering to specific policies and guidelines (service revocation, discipline, terminations, etc.).

Device security and controls

Provide a list of all control actions that may be applied to a device and the rationale for the control. Examples include:

- Device wipe after **xx** device passcode attempts



- Device lock after **xx** minutes requiring reentry of your passcode
- Device passcode change every 90 days, minimum length of **xx**, contain at least **xx** letters or numbers and enforcement of passcode history checking
- Device remote wipe when user leaves the company, device is lost, stolen, or compromised (jailbroken/rooted), or incorrect entry of the device passcode 10 times
- Vulnerability of personal data, and that the user is responsible for the backing up all personal information



Appendix B: Personal Device Usage Policies and Guidelines (Template)

Overview

The Company would like to provide greater mobile device choice to its knowledge workers and simultaneously reduce end-user mobile device complexity. Providing secured company email/calendar/contacts data, mobile applications and secure intranet access on employee personal mobile devices allow these employees to use the devices they prefer.

Purpose

The purpose of this document is to define the responsibilities, guidelines, and terms of use for employee-owned mobile devices configured for Company data use.

Definitions

1. **Mobile Device** – Employee-provided smartphone, tablet or laptop intended to be used to perform Company-related work activities
2. **Company Computing Resources** – Computer hardware, software, data and network resources used by the Company, including applications, intranet web access and Company email/calendar/contacts
3. **Users** – Employees, contractors, consultants, temporary workers, and other persons or entities authorized to use approved Mobile Devices to access Company Computing Resources
4. **Device Management** – Management, security, and monitoring of all Mobile Devices that access to Company Computing Resources

Scope

This document applies to employees who wish to access Company Computing Resources on a personal Mobile Device.

Personal Mobile Devices referenced in this document are limited specifically to those listed in the Approved and Certified Mobile Devices for BYOD.

Eligibility

The Company is making the Bring Your Own Device (BYOD) program available to Users who are willing to



agree with the policies and guidelines, and have a device that is listed in the Approved and Certified Mobile Devices for BYOD. CIO approval is required for Users with devices not listed in the Approved and Certified list or who wish to use more than one device to connect to Company Computing Resources.

References

1. *<Placeholder to links for other relevant User Agreements and Acceptable Use documents not specifically related to BYOD or Mobile Devices>*
2. Approved and Certified Mobile Devices for BYOD *<link>*.
3. Current Enforced Policies for BYOD Devices *<link>*.
4. Mobile Device Stipend Terms and Conditions *<link>*.
5. BYOD User FAQs *<link>*

Responsibilities

Information Technology Responsibilities

1. Information Technology (IT) is responsible for configuring and supporting the User's Mobile Device to access Company Computing Resources.
2. IT is responsible for smartphone system removal and performing a "remote wipe" of company data from a User's lost or stolen Mobile Device. In some situations, IT may perform a full device wipe after providing sufficient notice to the User to allow for personal data backup.
3. IT is responsible for smartphone system removal and performing a "remote wipe" of Company data from a User's Mobile Device upon termination of employment with the Company.
4. IT is responsible for maintaining a list of stipend-eligible employees and providing Accounting/Payroll access to that list.

User Responsibilities

1. The User is responsible for using Company Computing Resources on his or her personal Mobile Device within the same constraints as on a Company-owned device by adhering to all device and network acceptable use guidelines referenced within.



2. The User will not download or transfer sensitive business data to their Mobile Device outside of managed and approved mobile Computing Resources and applications.
3. The User will password-protect the Mobile Device.
4. The User must maintain the original Mobile Device operating system and keep the device current with security patches and updates, as released by the manufacturer.
5. The User agrees not to share the Mobile Device with other individuals or family members.
6. The User agrees to delete any sensitive business files that may be inadvertently downloaded and stored on the device through the process of viewing email attachments.
7. The User will not backup/download/transfer sensitive business data/documents to any third party service.
8. The User is responsible for contacting the IT Help Desk immediately in the event that their Mobile Device is lost or stolen.
9. The User is responsible for contacting the IT Help Desk immediately if they have replaced their Mobile Device.
10. The User is responsible for all Mobile Device support requirements, including the cost of repairs or replacement. The company is responsible, however, for configuring and supporting the Mobile Device to receive and access Company Computing Resources.

User Responsibilities (When Approved for Stipend)

1. The User is responsible for maintaining and paying the monthly/annual fee to the telephone mobile carrier. All mobile telephone charges that he or she incurs are his or her responsibility, regardless whether such charges are work related or for personal use. This includes, but is not limited to, charges resulting from texts, data plan surcharges, calls, navigation, or application uses or from early termination fees.
2. The User receiving a monthly stipend is responsible for notifying the Company immediately if he or she discontinues mobile telephone service so that the stipend can be discontinued.



Procedures and Security

Program Signup

Employees wishing to participate in the program must complete and submit a request, and agree by signing in the appropriate space on the form that they have read and understood this document.

Participating employees approved to receive a stipend must agree to the Mobile Device Stipend Terms and Conditions by signing and attaching the form.

Mobile Device Limitation

The Company allows one (1) personal device for Company Computing Resources access for each participating User. Additional licenses will be based on business need and will require CIO approval.

Mobile Device Restrictions and Controls

The Company may place various security controls and restrictions on your device. These include the enforcement of a passcode and limiting of device capabilities, such as device camera, access to cloud services and restriction of certain applications. Specifics on these policies can be found in the Current Enforced Policies for BYOD Devices document.

Accessing Company Computing Resources

1. As a prerequisite for accessing Company Computing Resources on a User's personal device, the User must first enroll their device in the Company Device Management system.
2. Once a participating employee enrolls their approved Mobile Device and the device is configured by the Device Management system, all corporate access and data will be managed and controlled by the Device Management system.

Jailbroken or Rooted Devices

1. Jailbroken Apple iOS devices and rooted Android devices pose a risk to Company data contained within the secure communications app. Therefore, the Company will disable or remove company data access on devices determined to be jailbroken or rooted.

Expectation of Privacy

The company will manage the configuration of the Mobile Device and, as such, will have access to information on the device including location, installed applications, data usage and other device related information.



User Acknowledgment And Agreement

It is the Company's right to restrict computing privileges, or to take other administrative or legal action due to failure to comply with the above referenced Policy and Rules of Behavior. Violation of these rules may be grounds for disciplinary action up to and including termination. I acknowledge, understand and will comply with the above referenced security policy and rules of behavior, as applicable to my BYOD usage of Company services. I understand that the Company is not responsible for any loss or theft of, damage to, or failure in the device that may result from use of third-party software and/or use of the device in this program. I understand that business use may result in increases to my personal monthly service plan costs.

Should I later decide to discontinue my participation in the BYOD Program or cease to become an employee of the Company or replace my Mobile Device, I will allow the Company to remove and disable any Company provided third-party software and services from my personal device. This may require a factory reset/full wipe be performed on my Mobile Device.

Employee Name: _____

Approved BYOD Device(s): _____

Employee Signature: _____ Date: _____



Appendix C: BYOD Policy FAQs (Sample)

MaaS360 is a mobile device management solution that has been implemented by the Company to provide visibility and control over mobile devices connecting to the corporate environment.

Using MaaS360, the Company can grant you access to corporate resources including email, intranet, VPN, campus Wi-Fi, Citrix or enterprise apps, while ensuring you meet corporate policies (e.g. having a device password). The Company may also distribute corporate applications and documents to your device using MaaS360.

In addition to helping you locate your device and protect corporate data on the device, Help Desk options like password reset and remote lock are also available. If your device is lost or stolen, it may be possible to recover it or remove only the corporate data if it cannot be located.

Using this technology, the company can protect its business while providing you access to valuable company resources. The following set of frequently asked questions will help you in understanding your responsibilities and what you can expect by participating.

Q. I would like to participate in the BYOD program. How do I get started?

A. First, review the supported device list and ensure that your device has the needed capabilities for the BYOD program, and then go to the enrollment URL provided and follow the instructions to enroll your device.

Q. I have been approved to use my personal device to access corporate email, provided I enroll my device. Why is this required and should I sign up?

A. Opting into the BYOD program and enrolling your device will allow you secure access to email, networks, applications and corporate documents. It will also allow the company to locate your device if it is lost or stolen and wipe corporate data if the device cannot be located.

Q. Will enrolling and allowing my device to be managed impact my device's performance and battery life?

A. It will use about 2-3% of your battery of the timespan of a full charge. This is less than popular traffic, music, and location-based social apps.

Q. What can the Company see with respect to my device after enrolling? Should I be worried about my privacy by allowing my employer to manage my device?

A. When you enroll in the BYOD program the Company will be able to report on certain aspects of



your device. The following table lists the information that can and cannot be viewed by a limited number of IT support team members.

Information	What the Company can see
Your phone calls, text messages and contacts	No visibility
Your pictures & videos	No visibility
Your personal emails accounts or emails	No visibility
Your purchased music, movies or books	No visibility
Your documents stored or created in Evernote, Dropbox or other third party apps	No visibility Note: The Company may have a directive that prohibits the movement of data from the corporate network to the cloud, so they may blacklist certain applications that enable this, such as Dropbox and Evernote.
Your data stored inside an app, such as Facebook or WhatsApp	No visibility Note: The Company policy may have a directive that prohibits certain social media activities and applications.
Your website visits when not using the company network	No visibility unless using the MaaS360 Secure Browser
Your location	Visibility is dependent on the Privacy settings within the MaaS360 platform. Ask the Help Desk for the setting for your device. Location may be hidden using the privacy settings on the device Note: If your device is lost, the location information may be important in its recovery.
Your personal applications	Visibility is dependent on the Privacy settings within the MaaS360 platform
Device hardware and security information	Can be viewed by IT and is necessary to manage the device



Q. What controls and actions will be applied to my device when I enroll?

A. There are a number of controls that may be applied to your device when you enroll which are intended to support security and acceptable use goals of the Company.

Control	Description
Device Passcode	<p>A device lock passcode will be enforced on your device requiring you to enter the passcode before the device can be used.</p> <p>Rationale: The passcode serves a dual purpose. Firstly, it is required to enable the encryption on the device to secure data. Secondly, it prevents unauthorized access to the device.</p>
Cloud Services	<p>Cloud services may be restricted or disabled.</p> <p>Rationale: The transmittal and storage of corporate information to third-party servers is prohibited. Applications such as DropBox and Evernote may also be blacklisted.</p>
Devices Operating System Upgrades	<p>Upgrades may be delayed until the new version of the OS has been tested and certified.</p> <p>Rationale: New device software may introduce vulnerabilities and data security issues. Upgrades may be prevented and/or discouraged, and performing an upgrade could cause your device to be out of compliance with Company policies.</p>
Device/Corporate Wipe	<p>If your device is lost, stolen, you opt out of the BYOD program or you leave the company, the corporate data on your device may be removed using a remote command.</p> <p>Rationale: Once the device is no longer managed, the Company must protect the data that may remain on the device.</p>



Control	Description
Locate	<p>If your device is lost or stolen, IT may use its GPS functionality to locate it.</p> <p>Rationale: Your device may hold sensitive Company data and locating the device is important. If the device cannot be found, it may be remotely wiped.</p>

Q. Are there any advantages for me personally if I enroll my device?

A. Yes, most MDM solutions offer an end user portal to allow you to lock your device, reset your password, locate or even wipe your device. Enrolling your device is a requirement in order for you to access other Company resources (e.g. email/calendaring).

Q. What type of data plan will I need?

A. The addition of corporate services to your device will not significantly increase your data usage, however, it is recommended that you closely monitor your data usage and make adjustments to your plan as needed. The company is not responsible for data plan overage charges and will not pay for them.

Q. What happens if I do not follow guidance or if I remove the management agent?

A. The company may temporarily or permanently revoke any email, VPN, and Wi-Fi profiles, applications and documents provided during the enrollment process if there is an indication that the device is not compliant. Removal of the device management application and management profiles will cause the device to revert back to a personal device with no corporate services enabled.

Q. Who do I call if I lose my device?

A. You are obligated to report a lost or stolen device to the Help Desk immediately. This will trigger a lost device process to attempt to locate the device.



Q. Who do I call if I need my device repaired?

A. The repair and replacement of the device is your responsibility, and any repairs must be facilitated and paid for by you. If the device is replaced due to a failure, it will require re-enrollment. The old device will be remotely wiped.

All brands and their products, featured or referred to within this document, are trademarks or registered trademarks of their respective holders and should be noted as such.

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