BYOD Policy Implementation Guide

Three simple steps to legally secure and manage employee-owned devices within a corporate environment

Absolute® Software

We won't bore you with the typical overview that speaks to the imminent arrival of BYOD and the advent of employee-owned devices on the corporate network. If you're reading this document, you know that BYOD isn't coming, it's already here.

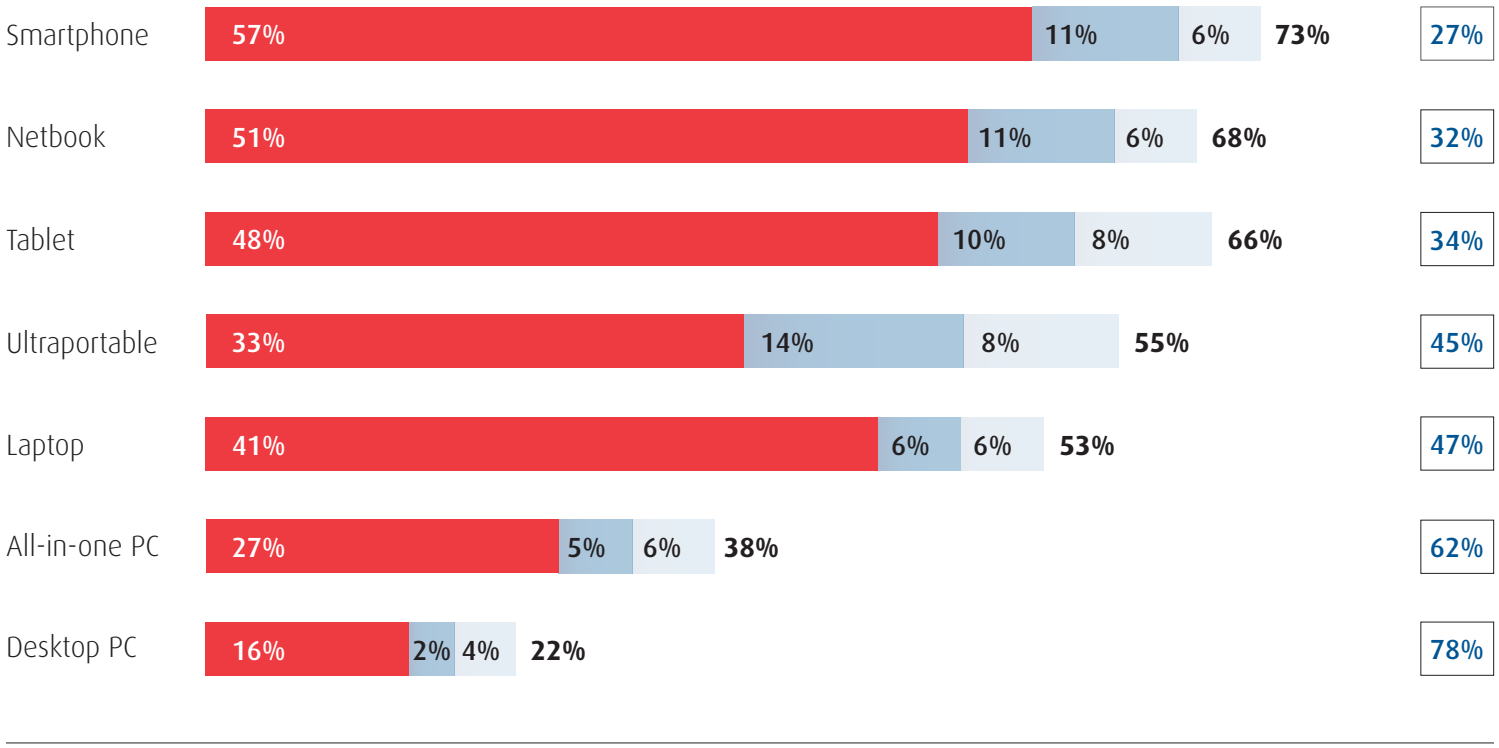
The purpose of this guide is to provide practical, concrete steps that allow you to efficiently incorporate employee-owned devices into your deployment while securing and protecting corporate infrastructure and data.

STEP 1 – DEFINE YOUR IT REQUIREMENTS

Devices & Form Factors

These are the form factors employees use based on the results of this Forrsights survey from Forrester Research, Inc. It shows the current trends among information workers when they are permitted to choose their own device for work, including the option to pay for some or a portion of the cost.

MANY NA/EU INFORMATION WORKERS CHOOSE WORK DEVICES THEMSELVES AND SPEND THEIR OWN MONEY



Base: North American and European Information Workers

Source: Forrsights Workforce Employee Survey, Q4 2011

FORRESTER®

To begin, you must select the types of devices and operating systems that you are willing (and able) to support. It is not possible to standardize management for mobile devices since each operating system and even the hardware itself can impact IT capabilities. For your Mobile Device Policy, here are baseline criteria to use for assessing operating systems and device types:

Security	• Built-in encryption • Identification of jailbroken or rooted devices • Enforceable passwords • Geolocation capabilities • Remote lock / wipe
Manageability	• An API that enables Mobile Device and/or Mobile Application Management • Extended MDM API via hardware vendor • Support of Exchange ActiveSync policies that comply to company standards
Apps	• A broad range of commercially available productivity apps • Support for developing and deploying your own custom apps • Availability of key apps specific to the form factor

Based on these criteria, you should be able to define the list of form factors and operating systems you will support.

Network Accessibility

Next, you must create an environment that will support employee-owned devices during the enrolment process. The simplest solution is to set up a guest wireless network that is separated from the internal network. This can serve as the enrolment network for employee-owned devices. Once enrolled, your MDM solution should automatically evaluate and assign privileges and restrictions based upon the policies you've created.

Basic privileges include access to company email, company Wi-Fi, and VPN configurations. These privileges should be tied to a policy that defines the security requirements of the company. Devices that do not comply with the security policy should be blocked. For instance: devices that are jailbroken, rooted or have blacklisted apps installed.

Provisioning access through your MDM solution benefits the organization and the employee:

- Employees receive access immediately
- IT doesn't need to manually provision devices
- Wi-Fi passwords are not shared with employees
- Remediation of future violations will be automatic since access is tied to the security policy

Management Policies

The final component for IT readiness relates to management policies and restrictions to employee-owned devices. This is broken down into three basic considerations:

Policy-based management: Employee information is already organized within directory systems such as Active Directory or Open Directory, including departments, geographies, and job titles. Save yourself a lot of time and base your device policies on these groupings.

Security: Create a baseline security policy that enables automatic remediation when devices fall out of compliance. Other criteria should be identified and implemented including company passwords and app blacklists.

Document Management: Unless you provide employees with a means to securely access corporate documents, they will invent their own. The best practice is to provide a centrally administered document repository that manages file availability by policy, while allowing IT to delete files as necessary. This is the best model to secure company data while respecting device ownership and user experience.

STEP 2 – DEFINE YOUR LEGAL REQUIREMENTS

The most significant challenge associated with BYOD is the balance IT must maintain between respecting the privacy of the employee while securing the corporate network and any data contained on the device.

Since this is essentially a collaboration between the employee and the organization, it's best to put it in writing:

Mobile Device Policy

This is a comprehensive document that should incorporate the specific requirements of your organization, based upon guidance provided by various internal stakeholders including general legal counsel, IT, Human Resources, employees and others.

Each policy is unique but generally should address some or all of these aspects:

Criteria

- Defines accountability and responsibilities
- Defines process for policy violation including consequences
- Focuses on a set of standards without including details such as device type and operating system
- Sets expectation that standards will be updated periodically

Users & Funding

- Defines how devices will be used by employees
- Defines how security requirements will be communicated to employees
- Whether a technology stipend program is needed and if so, who will pay
- If required, defines the reimbursement process for recurring costs to employees
- Support for contractors using their own devices on the corporate network

Legal Considerations

- Enforceable
- Whether regional or country data privacy laws will restrict security measures available to IT and consents required
- Rights to audit and monitor activity on personally owned devices and any limitations based on local laws and regulations
- The ability to distinguish liabilities between users and the organization for usage of features, licenses, apps, etc.
- Consent for the company to access the device for business purposes
- Sets out how to remove devices from the population and how sensitive data and company property are removed
- Obligations on employee to report loss of device and employer's right to wipe it

Human Resources

- Details of control over corporate information stored on employee-owned devices
- HR policies that can govern the use of personally owned devices for personal use during work and non-work hours or in a work or non-work environment

- Contract language to incorporate independent contractors and vendors and their compliance with the Mobile Device Policy
- Employee awareness and training
- Details of employee payment plan if the employer is initially paying for the device and employee is paying it down in installments

Employee Mobile Device Agreement

This is a simpler document with the sole purpose of acknowledging each employee's acceptance and agreement of the terms associated with the corporate Mobile Device Policy. By accepting the terms, the employee acknowledges that IT will have the legal right and ability to secure their device and the data it contains if required. See Appendix A for a sample of this agreement.

The employee opt-in is important in order to mitigate any future scenario where an employee may claim they were unaware of the policy. Since employee acceptance allows IT to perform security measures including the deletion of some or all data from a device and (depending on the nature of the corporate policy) potentially seizing a device, it's important that the company can prove its right to carry out this type of security activity.

Employee agreements should be preserved and available for future access as required.

STEP 3 – IMPLEMENT MDM SOFTWARE

Now that you have all of the internal requirements identified and in order, you need to select the appropriate software application that will allow you to properly manage and secure corporate- and employee-owned mobile devices.

Similar to the criteria you applied while assessing the different types of operating systems and form factors, you need to ensure the solution you select is able to deliver some baseline and supplementary capabilities:

Platform Flexibility	• Easily installs within the existing environment • Leverages existing security and network infrastructure • Minimal adaption required • Consolidation: Able to manage all IT form factors and operating systems via a single console (ideally to include desktop and laptop computers)
Administration	• Role-based administration so technicians can be assigned to specific user groups with defined management privileges
Mobile Apps Management	• Distribution of in-house and commercial apps • Apps management capabilities to support and automate user self-service • Support for the Apple ASVPP program (if you purchase Apple apps)
Security	• Application of multiple policies per device, for example an umbrella security baseline for all devices but separate privileges or restrictions per department or user role • Automated remediation of non-compliant devices • Secure document distribution and management • Remote freeze and wipe capabilities • Enterprise password support

ABSOLUTE MANAGE FOR BYOD

Absolute® Manage for mobile devices has successfully automated the employee workflow associated with BYOD.

This allows IT administrators to forego the manual process of enrolling employee-owned devices and collecting the individual agreements acknowledging each employee's acceptance of the Mobile Device Policy terms. Here's how it works:

1. At point of enrolment, the employee will receive a prompt on their device asking if the device is owned by the company or the employee.
2. If the device is owned by the employee, the Employee Mobile Device Agreement will appear on-screen. The employee must read the agreement and select "Agree" in order for the enrolment process to proceed.
3. A confirmation email is automatically generated to the employee confirming their acceptance of the terms and providing them with more information about the company's Mobile Device Policy. This email can include a copy to Human Resources for each employee's file.
4. Once the device is identified as employee-owned, policies and profiles tailored for BYOD can be automatically and instantly enabled and loaded onto the device.

Absolute Manage is a lifecycle management and mobile device solution that allows IT administrators to manage PC, Mac®, iOS, Android, and Windows® Phone devices from a single console. Customers can remotely engage with their deployment and perform standard maintenance routines as well as take strategic and responsive measures based upon the requirements of each device.

For more information about Absolute Manage for mobile devices, visit:
www.absolute.com/mdm

EMPLOYEE MOBILE DEVICE AGREEMENT

This is a legally binding and enforceable agreement. In exchange for allowing you to use your personal device in our corporate environment; you agree as follows:

Acceptance of this agreement is a condition to your being allowed to use your personal device in our corporate environment, and you agree to abide by the Company's Mobile Device Policy (URL TBD) and any amendments from time to time. The Mobile Device Policy forms part of this contract.

If your device is lost or stolen, you must notify (TBD) immediately by email (TBD) or telephone (TBD) to report the loss.

Things you should know:

-The Company may access all information, applications, and data stored on your personal device while it is enrolled. You irrevocably consent to such access in accordance with the Company's Privacy Policy until your personal device is de-enrolled from the program.

- The Company has the authority to remotely wipe data on personal devices (and personal data if necessary) should the need arise, including for security reasons or if employment is terminated by either party.

- In case of violation of the Company's Mobile Device Policy, the organization may take any or all of the following steps, among others:
    - Special training to help you understand security measures
    - Loss of mobile device privileges
    - Surrender of device and/or remote wiping of the device
    - Termination of employment

This device must remain compliant with the Company's Mobile Device Policy to continue to be allowed access to the corporate network, email, contacts, and other corporate information.

If you wish to no longer use your personal device in our corporate environment, you must contact (TBD) to have the device removed. The company may delete all information on your personal device prior to removing your personal device from the program.

(Agree) I have read and understood the Company's Mobile Device Policy. I agree to these terms and wish to proceed with the enrolment of my personal device.