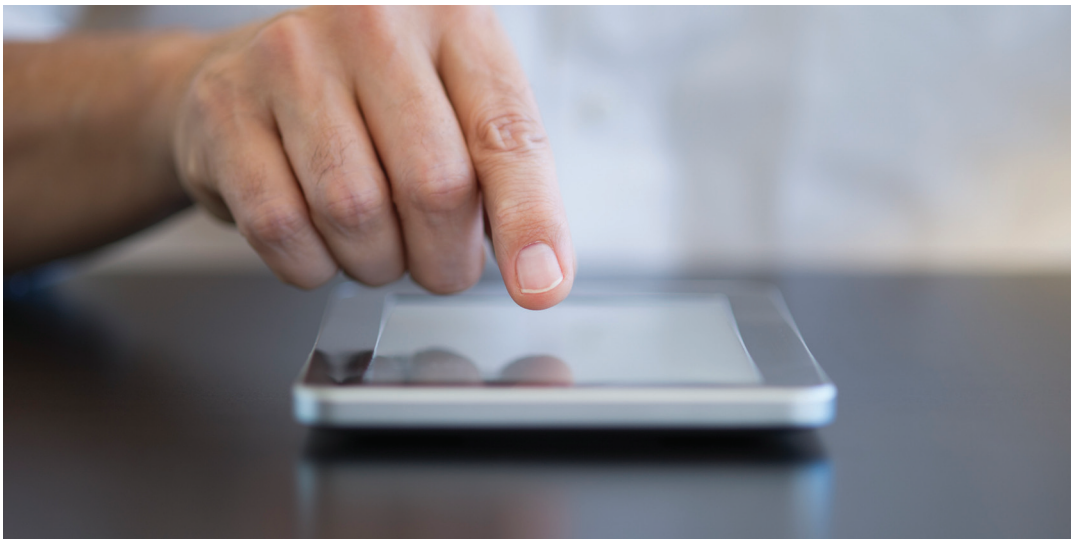
ZENPRISE
Protecting Mobile Enterprises
Everywhere

Go Ahead, BYOD. Make My Day.
Zenprise Policy Template



The BYOD phenomenon

Even though the transition of mobile phones into computers has been a long time coming, the sea change in the past couple of years is dramatic: Consumer mobile devices that are so compelling to business users that we are willing to upend the "way we do things around here" to have them in our workplace. Just a couple of years ago, the iPad didn't exist and the notion of employees using their personal smartphones for corporate email and apps was laughable. Now, according to Forrester, nearly 60 percent of organizations are embracing a "bring your own device", or BYOD, program. And that number is growing every day.

Whereas enterprise mobility used to mean that an elite few—often executives and salespeople—received company standard-issue BlackBerrys for their mobile phone and email, BYOD is an equalizing force in that now a far greater swath of employees are allowed to bring their smartphones and tablets (and in many cases, both) and attach to the corporate network. And why wouldn't you want them to go mobile? Untethered employees are happier and more productive on-the-go. But just as Dirty Harry confidently stands up to the bad guys, you need to have the confidence in your mobile security and management to be able to say to those consumer devices: "C'mon, make my day."

The risk

Giving employees access to corporate resources from their smartphone or tablet is a risky proposition. Unlike standard-issue, locked-down PCs or tightly controlled BlackBerrys, mobile devices in today's enterprise are diverse, have varying levels of vulnerability, and offer no consistent way for IT to manage even the most basic device security features. From their devices, employees can access your network, business applications, and your most sensitive business data whenever and wherever they want to. What if they don't have a passcode enabled and leave their device at Starbucks? What if they're synching non-public financial data using Dropbox? What if they're logging into your salesforce automation tool over an insecure wireless network at the airport? What if they're downloading non-compliant or inappropriate games or apps? What if they leave the company but still have your business apps and data on their devices? These are just a few examples of how BYOD can jeopardize sensitive data and expose the enterprise to mobile threats.

The BYOD management challenge

Beyond security and compliance, simply managing BYOD is a hairy process. Even before you roll out a BYOD program, you'll need to figure out which devices you'll support, and for whom. And how you'll enforce that policy. You'll have to think about which apps you'll make available (now and in the future) to groups of users, how you'll provision those apps, how you'll ensure users have the correct versions and applicable patches, and how you'll ensure service levels.

Then when you actually start the program, you'll need to figure out how to onboard, offboard, and make changes to mobile users and devices. Given how dynamic the mobile market is, with rapid device adoption, turnover, and an increasing ratio of devices-to-users, it makes sense to map your mobile users to your user directory (e.g., LDAP) so you don't have to manually update your mobile system every time an employee joins, departs, is promoted, or changes groups.

You'll need to find a way to set policies, map them to users and devices, and easily change them when your business needs change. You'll need to monitor and support the devices, both proactively (e.g., keeping an eye on device statistics and application performance) and reactively (e.g., locking or wiping a device upon its loss or theft). You'll need visibility into your mobile network and compliance status, and the ability to see your mobile devices alongside the rest of your IT assets by integrating with corporate security information and event management (SIEM) solutions.

ZENPRISE
Protecting Mobile Enterprises
Everywhere

What's needed is a mobile device management solution that secures the mobile enterprise end-to-end, while simplifying deployment, ongoing administration, and the end-user experience.

Zenprise: Solving security and management

With cloud-based and on-premise offerings, Zenprise lets your IT professionals secure and manage the most comprehensive array of mobile devices, gain visibility into and control over mobile apps, and shield the corporate network from mobile threats.

Zenprise offers your organization:

- Security for your mobile enterprise, across devices, apps, the network, and data;
- The most intuitive and easiest-to-manage MDM solution in the market;
- An enterprise-grade architecture, with security built in and high availability at all tiers;
- The most comprehensive global services, support, and training among all MDM vendors; and
- Flexible deployment options: On-premise, cloud, or hybrid solutions

As you implement a new BYOD program or even fine-tune your existing one, below is a policy template for getting employee-owned devices under control. Based on Zenprise customer best practices, this template serves as a starting point for helping you secure and manage your BYOD environment while enabling your users to be more productive on-the-go.

	POLICY	CONSIDERATIONS	BEST PRACTICES
✓	**Device platform and OS version.** *Specify which device platforms and OS versions you will support.*	• Which device platforms best support your mobile objectives? • Are there device platforms or OS versions that lack features you require?	• If you are rolling out BYOD, discover what devices are connecting now and use that as your starting point. • Exclude devices that lack features you require, unless you can compensate another way. • Report fully on device platform and OS, as well as on your actions against potential violations. • *According to Aberdeen, "best in class" organizations support an average of 3.3 platforms*[1]
✓	**Pre-enrollment device check.** *Prior to enrollment, conduct a device compliance check.*	• Based on what parameters will you block devices from your network? • Do any of the above parameters cause risk to your corporate network or data upon initial device enrollment?	• Enforce a pre-enrollment device compliance check to block jailbroken or rooted devices. Such devices can contain threats and vulnerabilities that can expose your network even before you deploy policies to them. • Deploy policy packages only on devices that adhere to your device platform/OS version policy. • Report fully on your pre-enrollment check, as well as on your actions against non-compliant devices.
✓	**User agreement.** *Be explicit and gain their agreement on your role in managing, securing, monitoring, and retiring mobile devices.*	• What kind of device management and monitoring do you need to do to ensure your corporate network and data security policies? • Do you intend to remotely control the device at any point for the purpose of IT support? • Do you intend to monitor any mobile communications? • Regardless of your policies on your non-mobile and corporate-owned IT infrastructure, users often have a greater expectation of privacy on both mobile and personally-owned technology, even if they're using it for business purposes.	• Set and **communicate** your policy about how you will manage and monitor devices while users are enrolled, including any communications monitoring, even if similar to your other communications policies. Also be clear about how you will decommission both company-issued and BYOD devices upon employee departure, and what that means for their personal data. • Gain employees' **explicit employee agreement** with the policy upon provisioning their device access; encourage them not to store personal content on company-issued devices. • Develop a process about which business data and apps you will remove/revoke access to upon employee departure. Apply it consistently for BYOD devices.
✓	**Device management by ownership.** *Separate and manage company-issued devices differently from BYOD ones.*	• Do you have different access policies for company-issued and BYOD devices? • Do you have different processes for company-issued and BYOD devices when dealing with lost, stolen, or decommissioned devices?	• Create a single point of truth for device ownership in your system. • Auto-tag devices as company-owned or BYOD by importing device IDs from an asset or configuration management database. • Do not let users self-identify whether their device is owned by them or the company, as doing so obviates reporting integrity.
✓	**Setting and enforcing passcodes.** *Enforce passcodes on all mobile devices on your network.*	• How complex should your passcode be? • How often should you force users to change their passcodes? • Should you set a maximum for passcode failed attempts, and what should the consequence be?	• Set and enforce passcodes on all mobile devices on the network. Block devices whose passcode settings are out of policy. • Trade off passcode complexity based on ease-of-use versus risk of inappropriate mobile access. • Block devices from the network whose passcode settings are inadequate or out-of-date. • Report fully on your passcode enforcement, as well as on your actions against potential violations. • *Passcodes are the most commonly deployed policy, according to the Zenprise Mobile Device Management Cloud Reports.*

[1]Aberdeen

	POLICY	CONSIDERATIONS	BEST PRACTICES
✓	**Encryption of data at rest.** *Enforce encryption of data at rest for all devices with corporate data on them.*	• Is your organization subject to regulatory or industry policies that require or suggest encryption of data at rest, or in which encryption satisfies breach notification? Examples include HIPAA, GLBA, PCI, and SOX.	• Set and enforce encryption of data at rest. • Use industry-standard encryption standards and protocols. • Block devices that do not have encryption enabled from the network. • Report fully on your enforcement of encryption of data at rest, as well as your actions against potential violations.
✓	**PKI and certificates.** *Set and enforce use of PKI and certificates.*	• Do you have a PKI system such as Microsoft Certificate Authority? • Do you use certificates for two-factor authentication and SSO?	• Use PKI and certificates for strong user authentication and SSO for network and application access.
✓	**Wireless network access.** *Set and enforce corporate WLAN access; set security requirements for public WLAN access.*	• Will your employees have access to your WLAN via their mobile devices? • Can your WLAN accommodate the added load from personally-owned smartphones and tablets? • Will you be able to extend certificate-based WLAN single-sign-on to smartphones and tablets? • Will users be accessing your network from unsecured WLANs?	• Enforce corporate WLAN access when on-premises to save data cost and device battery, speed up network access, and benefit from added security, authentication, and SSO. • Specify and enforce connection via your corporate access points for compliance and load management. • Report fully on your enforcement of your wireless policy, as well as your actions against potential violations.
✓	**Virtual private network access.** *Set and enforce VPN access.*	• Will your employees be accessing sensitive business apps or data via their mobile devices? • Will you be able to extend certificate-based VPN SSO to smartphones and tablets?	• Enforce VPN connectivity for encryption of data in transition for app traffic between devices and the corporate network. • Deploy VPN certificates on mobile devices for added authentication and SSO. • Report fully on your enforcement of your VPN policy, as well as your actions against potential violations.
✓	**Mobile app access.** *Grant granular app access and secure app communications.*	• Do you have critical business applications that you want to segregate from other consumer apps on the BYOD device? • Do you want to offer access app-by-app? • Do you need to encrypt app traffic end-to-end? • Do you need to ensure app performance and reliability for certain apps?	• Identify, segregate, and secure critical business apps and their communications with application-specific VPN-like tunnels such as Mobile App Tunnels. • Report fully on your enforcement of mobile app access policy, as well as your actions against potential violations.
✓	**Mobile app restrictions and compliance.** *Lock down unwanted or non-compliant apps.*	• Are there certain apps that you don't want to even launch on the device? • Are there certain apps or device resources that you don't want users to employ while they're at work?	• Restrict malicious or non-compliant apps by restricting or locking them, such as via Mobile App Lock. • Restrict non-compliant or unproductive apps or device resources during business hours or on work premises with Dynamic Defense context-aware policies. • Report fully on the apps you're locking, as well as on your actions against potential violations.
✓	**Application enforcement.** *Blacklist and whitelist applications.*	• Has your organization identified mobile apps that are malicious or out of compliance with your policies? • Are there mobile apps that you consider unproductive or unrelated to the work at hand?	• It is unlikely that employees will tolerate mobile app whitelisting on their own devices. • It is unlikely that employees will tolerate mobile app blacklisting on their own devices unless the apps are malicious or truly non-compliant. • Blacklist only the apps that are malicious or truly out of compliance. • Report fully on which apps are on your blacklist and whitelist, as well as on your actions against potential violations.
✓	**Sensitive content.** *Control access to sensitive content via a secure content container on the device. Set mobile data leakage prevention policies.*	• Do you need to distribute sensitive content (presentations, documents, videos, etc.) to large numbers of users via their mobile devices? • Do you need to control whether users can save, print, email, and copy/paste for certain kinds of content? • Do you need to version-control and/or time-expire content? • Do you need to take automated action (e.g., wipe) based on context (e.g., device jailbreak)?	• Use the secure container on users' device to distribute content to them depending on role-based privileges, type of content, and context. • Set and enforce restrictive enterprise mobile data leakage prevention policies (e.g., block email, save, print, etc.) for sensitive content such as non-public financials or sensitive HR videos. • Set permissive policies for non-sensitive content such as sales collateral. • Use the secure container controls to time-expire content that you do not want to live after a certain date and version-control content that needs to be updated. • Set context-aware policies to wipe the container of all data should the device become compromised (e.g., jailbroken) or should an unauthorized party attempt to access the device (e.g., threshold of failed logins). • Report fully on your handling of sensitive content, as well as actions such as auto-wipe for compliance purposes.

	POLICY	CONSIDERATIONS	BEST PRACTICES
✓	**Telecom expense optimization.** *Set voice and data roaming policies.*	• Does your organization assume the wireless service expense for employee-owned devices?	• Disable data and/or voice roaming for certain classes of users. • Set policy deployment parameters to avoid data-intensive activities when users are roaming.
✓	**Device loss or theft.** *Lock and/or wipe the mobile device upon loss or theft.*	• Is your organization subject to regulatory or industry policies that require access control and monitoring? Examples include HIPAA, GLBA, PCI, and SOX. • Have any employees downloaded confidential company data onto the device that could be accessed if found by a third party?	• Set and communicate a policy/process for users to notify you upon device loss and theft. • Set and enforce a policy for the device to auto-lock after a period of inactivity. • If a device is lost, have a process in place for IT to lock it and re-set the passcode. • Set and enforce a policy for the device to auto-wipe after a threshold of failed login attempts. • If a device becomes stolen, have a process in place for IT to remotely fully wipe the device. • Report fully on this process and your steps for remediation for compliance purposes.
✓	**Employee departure.** *Decommission devices upon employee departure.*	• Does your organization support both company-issued and BYOD devices? • Is there likely to be sensitive corporate data or personally-identifiable data on users' mobile devices? • Are you subject to regulations that would require you to disclose publicly or to customers, or would levy a monetary fine on your organization, if a mobile data breach were to occur as a result of data saved onto a departing employee's mobile device? • Do employees use their company-issued devices for personal activities?	• Per the prior practice in the enrollment section, communicate and gain employees' agreement on your device decommissioning process, including the potential for you to wipe their device of all data—corporate and personal. • Develop a process about which business data and apps you will remove/revoke access to upon employee departure. Apply it consistently for BYOD devices. • If your policy is to fully wipe a company-issued devices upon employee departure, consider the possibility that employees have personal data on the device (e.g., pictures of their children). Under certain circumstances, consider allowing them to transfer personal content prior to device wipe. • Consider performing the "selective wipe" action on departing employees' devices. This will wipe their device of corporate profiles, applications, and email, leaving their personal apps and content intact. • Consider enacting an administrative setting that prohibits administrators from performing full wipes on devices. • Report fully on device decommissioning process for compliance purposes.

The above policy checklist is just the tip of the iceberg. As you strategize how you will roll out mobile access, deploy apps, and govern your mobile users, consider investing in a professional services engagement to help you identify and deploy your mobile policies. Zenprise offers a Mobile Policy Implementation package, a professional services engagement that helps you identify the goals and business risks that will drive your policies, map them to Zenprise product policy definitions, gain your approval, and then implement the policies in a manner that's as non-disruptive as possible to your business.

Now that you have a rough overview of the security and management challenges associated with BYOD and a set of BYOD policy recommendations gleaned from our customers, support team, and product experts, you are now armed (or—taking a Dirty Harry approach—you're now armed and dangerous!) to take on BYOD.

About Zenprise

Zenprise is the leader in secure mobile device management. Zenprise MobileManager® and Zencloud™ let IT say "yes" to personal and corporate-owned mobile devices without sacrificing security and compliance requirements. Only Zenprise protects the mobile enterprise end-to-end with the industry's easiest-to-use MDM solution. This lets executives take their businesses mobile, gives IT peace of mind, and makes employees more productive on-the-go. Zenprise's extensive list of global customers and partners spans a cross-section of countries and vertical industries including: aerospace and defense, financial services, healthcare, oil and gas, legal, telecommunications, retail, entertainment, and federal, state, and local governments.

ZENPRISE

1600 Seaport Blvd, Suite 200, Redwood City, CA 94063
32 Rue des Jeûneurs, 75002, Paris, France

W +1 650 365 1128
W +33 1 5325 0640
F +1 650 365 1118
WWW.ZENPRISE.COM