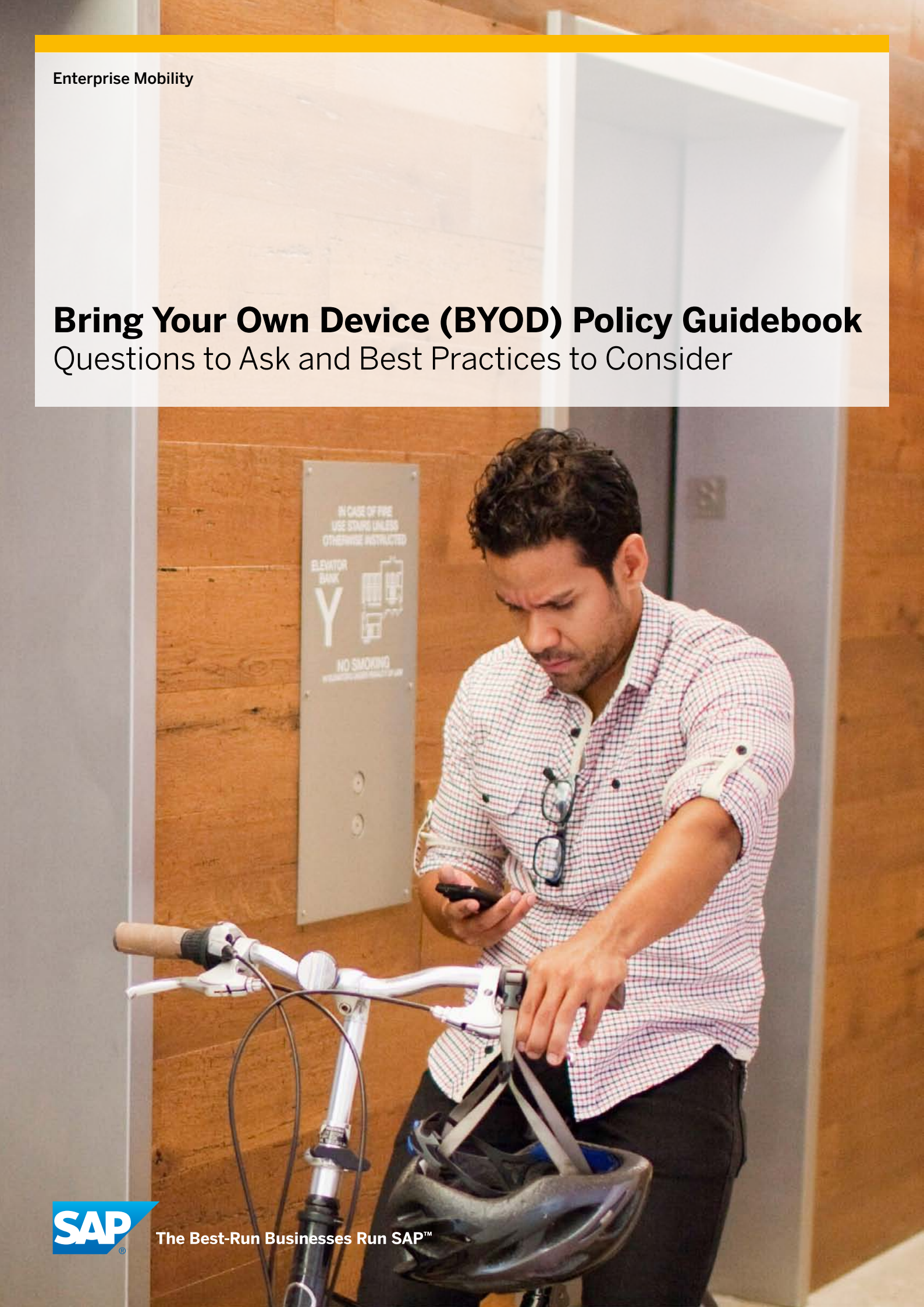
Enterprise Mobility

Bring Your Own Device (BYOD) Policy Guidebook

Questions to Ask and Best Practices to Consider



SAP

The Best-Run Businesses Run SAP™

Table of Contents

OBJECTIVES AND LEGAL DISCLAIMER

Whether yours is a large multinational organization, a midsize regional company, or anything in between, you should consider implementing bring your own device (BYOD) policies that meet your company's specific needs. Any decisions about your policies should be made by your executive management, IT, HR, finance, and legal teams. It is important that your decisions fit your company needs, meet your financial goals, and consider the security, legal, regulatory, tax, and other requirements that exist in the countries where you do business.

This policy guidebook is intended to answer common questions and help you through your policy development process. It should not be considered legal or financial advice. Samples provided are examples only.

SAP disclaims any and all liability for the use of this document and/or the considerations outlined herein, either in whole or in part, in the definition and/or application of specific policies by any company.

Introduction: How to Approach a BYOD Program

Your employees want to use their own mobile devices for work. This represents a tremendous opportunity for you to extend the benefits of mobile technology to all employees. As more companies embrace the bring your own device (BYOD) model, many questions arise. This policy guidebook was created to assist SAP customers in their BYOD implementations. It is intended to help guide you through the questions to ask and provide some best practices to consider when establishing your own policies.

Many of the recommendations in this guidebook are from SAP's Global IT department. This team has managed BYOD implementation for thousands of SAP employees around the globe and has firsthand experience answering these questions.

There are many basic questions to answer before you begin fully investigating a BYOD program for your company. Addressing these questions will form a basis for how to proceed with other stakeholders.

BEFORE YOU BEGIN

Q: What is your mobile strategy?

A: Before diving into a BYOD strategy, you may want to think about what mobile means for your business. Is it simply about accessing e-mail and calendars from a mobile phone? Is it about fundamentally transforming the way you do business? Mobile technology can mean many different things to different companies and can provide new avenues of connecting with your employees. Consider how you can innovate and discover new ways to do business and how this may impact your device ownership model.

Q: Will you vary the level of access to company data based on who owns the device?

A: A BYOD strategy is not the single answer to addressing the "consumerization of IT" trend. Consider the "corporate owned, personally enabled" (COPE) model. Regardless of who owns the device, corporate data and personal data need to be managed separately, and corporate data should remain under enterprise control. If you will restrict access for personal devices versus corporate devices, consider changing who can access specific applications or data.

Q: Which employee groups are eligible to access enterprise data?

A: Eligibility depends on your business needs and employee requirements. Employees who are task focused, such as field inspectors or service workers, are typically provided a corporate-owned device. Employees who do not require a mobile device for their job but can benefit from access to company data are prime candidates for BYOD. Consider creating a map of all employee groups and determining if you will restrict access to company data based on role, geography, management level, or other factors.

Q: What devices will you support?

A: Adopting a BYOD or COPE policy does not mean that you will support whatever mobile devices your employees want. A good long-term strategy will include compiling a short list of devices that meet your security requirements. Remember that a BYOD strategy may not be simply about providing access to e-mail and calendars. It is about enabling enterprise mobility and productivity for all. Consider your mobile application strategy and select devices that map to your long-term plan.

KEY QUESTIONS AS YOU BEGIN

Be sure to clearly define:
- Who is eligible to use a personal device
- What level of data employees can access
- Which devices are approved for use

Key Stakeholders and Their Considerations

In this section we will review the various stakeholders involved in a BYOD decision and address some of the areas that you should consider.

LEGAL CONSIDERATIONS

Often the first stakeholder you should connect with when defining your BYOD plan is the legal department. Consider the following questions.

Q: How can local privacy and data protection laws and regulations impact a BYOD strategy?

A: Allowing access to corporate data on a personal device means that you will be exposed to privacy laws. These laws vary significantly around the world and are intended to protect the employee. Countries in the European Union have the most restrictive privacy laws and regulations and can impact your ability to roll out a BYOD initiative as well as your approach to implementation in that region.

Q: How can you avoid starting from scratch in every country?

A: Approaching a BYOD policy should be done country by country. However, that does not mean that you need to start over each time. Start with the country in which you do the majority of your business or with the countries with less restrictive privacy laws and regulations. When expanding to new geographies, adapt your contracts to work in that region.

Q: What kinds of contracts should be created by legal?

A: We recommend that you put together two core documents: an electronic consent form and an acceptable-use policy. Samples may be requested from your SAP account team. You may already have a code of business conduct in place that addresses expected conduct.

HUMAN RESOURCES CONSIDERATIONS

The HR team is a key stakeholder when considering the BYOD approach and can act as a central awareness channel with employees.

KEY STAKEHOLDERS

Key stakeholders in BYOD policy decisions include:
- Legal
- Human resources
- Finance
- IT
- Corporate communications

Q: How does a BYOD policy affect onboarding and offboarding processes?

A: HR plays a crucial role as the liaison between the company and IT resources. IT needs to work with HR to ensure that proper processes are in place to activate devices for approved employees and also to establish proper dismissal processes. Existing processes can be used as a model.

Q: How should employee training and awareness be handled?

A: As part of the typical onboarding process, HR can provide basic awareness and education on device enablement, as well as education around user responsibility. Any technical questions can be handled by the IT department.

Q: How do I handle employees accessing unapproved applications from their device?

A: The acceptable-use policy discussed in the "Legal Considerations" section should satisfy this concern. Enterprise mobility management (EMM) tools can also be used to inventory applications on a user's device; however, IT may want to consider not using this function for personal devices while allowing it for corporate devices.

Q: What happens when someone chooses to leave the company or is terminated?

A: Since a device is personally owned, it will not be returned to the company upon departure. You have the ability to selectively wipe corporate data, or in the case of termination, you can wipe the device ahead of time. Ensure that your policies are clearly understood by employees. No one wants to have his or her device wiped when expecting only corporate data to be removed.

Mobile technology can mean many different things to different companies. Consider how you can innovate and discover new ways to do business, and how this may impact your device ownership model.

FINANCE CONSIDERATIONS

Often companies think that a BYOD strategy will save them money by passing the cost of hardware and even monthly service to the user; however, there are many more cost-related questions to address. The finance department is interested in ensuring that costs do not escalate.

Q: Who pays for the device and repairs?

A: Typically the employee pays for the full cost of the device and any maintenance or repairs. They are also responsible for replacing the device in the event that it is lost or stolen.

Q: Who pays for the voice and data plan?

A: Voice and data plans can be approached in many ways. Often companies will consider a stipend (monthly allowance) to contribute to the corporate portion of the plan. Other companies will fully fund the plan, while others vary their approach based on specific user groups (such as executive, manager, and employee). Some companies offer no reimbursement. Note that multiple plans for both a phone and a tablet can add significant costs. Some companies fund Wi-Fi-only tablets or allow employees to tether their tablet to their mobile phone plan. In general, we recommend that reimbursement should be capped to avoid costs getting out of control. It is also important to consider country-specific topics, such as tax regulations, contracts with local carriers, and so on.

Q: Who pays for roaming charges when an employee travels?

A: Roaming costs are a significant worry for telecom expense management and should be controlled. A telecom expense management solution that is part of your EMM solution should be leveraged to avoid this risk. When employees' devices are roaming, you can be proactively notified and can communicate with the user to avoid high billing.

Q: Should your company offer reimbursement for iTunes purchases?

A: Many companies do not formally allow purchase and expensing of individual apps via iTunes. With Apple's bulk purchasing program, it is possible to purchase apps for corporate distribution and manage them via your EMM tool. This licensing plan can benefit a broad group of employees and can increase adoption and employee satisfaction. In the case of one-off apps that are required for work, you may approve this expense at a manager's discretion.

KEY QUESTIONS ABOUT REIMBURSEMENT

Be sure to clearly address:
- Which devices are eligible
- Conditions for reimbursement
- Reimbursement limitations
- Monthly stipend amounts and maximums

Q: Should you offer reimbursement for accessories?

A: Accessories related to a personal device are usually the responsibility of the employee.

Q: Who pays for support?

A: Support is commonly a community-based approach with up-front support offered via self-service wikis and internal champions. Corporate apps and e-mail and calendar software that you have issued should be supported by IT.

IT CONSIDERATIONS

The IT department typically handles the bulk of the management of a BYOD implementation. There are many areas to consider, which are broken down here into the initial rollout, security, and mobile apps.

Initial Rollout

Q: What type of devices and operating systems should be supported?

A: Your short list of approved devices should include the popular enterprise-ready devices that your employees are asking for. You may choose to approve specific devices or specific operating systems as long as they meet your baseline security requirements. For example, choose to support iOS version 4.0 and later or Android version 2.3 or later. Base your decisions on the manageability of that operating system, and be sure that it ties in to your applications strategy. Consider that popular devices vary from country to country.

Q: How should you handle jail-broken or rooted devices?

A: Using an EMM tool like the SAP® Afaria® mobile device management solution, a jail-broken device can be detected and an action can be completed. For example, the corporate data can be automatically wiped or simply reported to management for an alternate action. Communication is key: your policy should clearly state that jail-broken devices will not be permitted to access corporate assets.

Q: How should you manage initial device rollout?

A: Utilization of an EMM self-service portal and internal wiki pages are recommended. A simple setup document can be distributed to speed the setup process. When needed, a local "mobile champion" can be approached to aid with setup in local offices.

Q: Should you start with a pilot?

A: Starting a BYOD project with a small test group is an excellent way to get started. You'll learn the common questions your users will ask and be able to test your policies on a range of employees. Be sure your trial group comes from a variety of departments and levels.

Q: How can you ensure compliance with your BYOD policy?

A: You can restrict access to corporate resources until users are compliant. Typically this is done via IT using an EMM tool (like SAP Afaria). Access to company data is restricted, but personal use of the device is not affected.

Q: How can you control when users install OS upgrades?

A: There is currently no ability to block OS upgrades on Apple devices, which can pose a challenge when you want to ensure that your apps work on the latest release. However, it is possible to restrict end-user access to corporate data if the OS version is below a specific level. Encouraging employees to wait a few days after an OS update will provide IT the time to test applications before updating. Communication is critical to ensure that users are not blindsided by apps that stop working.

Security

Q: How should personal devices be secured?

A: Using an EMM tool like SAP Afaria will ensure that you can fully secure both personal and corporate devices. For more information on this product, please visit www.sap.com/mobile/afaria.

Q: If an employee reports a lost device, should you wipe the entire device or only corporate data?

A: Typically companies take a phased approach to dealing with a lost device. You can start with a remote lock via a self-service portal. In the event the employee finds the device, it will not need to be wiped. If after a couple of days the device is not recovered, a full or selective wipe can be issued. The selective wipe will only remove the corporate data, but users may want personal data wiped in some situations.

Q: Is it possible to turn off GPS tracking?

A: Some companies like to be able to track where employees are at all times for a variety of business reasons. This may be a privacy issue in some areas. Using an EMM tool like SAP Afaria, IT has the capability to turn off tracking features for personal devices.

Mobile Apps

Q: How should you make apps available to users?

A: There are several options to make publicly available and corporate apps available to your users. You can set up role-based profiles for app distribution, ensuring that people get only the internal apps that they are entitled to. You can implement a private app store to distribute without the need to go through a public store like Apple's App Store or the Google Apps Marketplace.

Q: What kind of applications should you deploy to personal devices?

A: A BYOD policy offers the opportunity to enable enterprise mobility for all employees across the company. There are incredible opportunities to build internal applications to enable significant productivity gains. Simple workflows like vacation requests and approvals, purchase order approvals, expense reports, and so on can offer opportunities to speed business and save money. There are many types of applications that can be built or purchased. Consider this when defining which devices make your short list. Building apps for two to three standard operating systems will enable you to reach a broad audience and simplify development efforts.

Q: Should you allow employees to use Dropbox or other cloud-based file-sharing technologies?

A: Cloud-based file-sharing technologies are inherently insecure. Be aware that such services may put your corporate data at risk. Consider a document management system that is part of your secure EMM tool. Also consider disallowing backup to the cloud for the same reason.

Q: Where do users go for support of mobile apps?

A: You should support applications that you have developed for your employees. Outside of that, device, OS, or noncompany apps should be supported by the carrier, the application provider, public forums, wikis, and so on.

KEY EMPLOYEE POLICY ISSUES

Be sure to clearly address:

- Action taken for jail-broken or rooted device
- Process for reporting lost or stolen devices
- Actions to be taken when an employee leaves the company
- Support mechanisms and expectations
- Disclaimer for any liability for loss of personal applications or data

Q: What happens if an employee's personal device is lost?

A: Most personal device replacement programs provided by the carriers are very good. Loaner devices are typically not needed.

Q: Should I set and enforce use of a whole device password?

A: Passwords are a critical basic security requirement and can be enforced with your EMM tool. We recommend that you always enforce whole device passwords to protect both personal and corporate data.

Q: Should you limit use of cameras, Bluetooth, or other applications and services?

A: Depending on your company policy, you may restrict use of camera or Bluetooth with your EMM tool. EMM tools cannot control applications that they were not responsible for installing, but they can block access to all corporate resources if specific applications are present on the device.

Often companies think that a BYOD strategy will save them money by passing the cost of hardware and even monthly service to the user; however, there are many more cost-related questions to address.

Communication Challenges

Communication to your employees is a critical function when rolling out a BYOD strategy, since it typically involves new policy creation and violations may be unexpected.

Q: What level of executive buy-in is required?

A: Ensuring that you have senior-level executive buy-in is a critical aspect of your BYOD program. Before beginning, ensure that you have full support. You should rely on your executives to communicate the program to employees.

Q: How important is it to communicate the launch of a BYOD program?

A: Communication is very important, as it demonstrates your responsiveness to employee requests. A BYOD program is often considered good PR for the IT team and is generally perceived as a benefit by the employees. It is important that your communication be rolled out regionally via your executive team.

POLICY VIOLATIONS

Your policies should be very clear on consequences of violation, and any differences in consequences should be based on the type of violation.

Starting a BYOD project with a small test group is an excellent way to get started. You'll learn the common questions your users will ask and be able to test your policies on a range of employees.

Conclusion: Key Takeaways

A decision to implement either a BYOD or COPE model involves many stakeholders and decisions. Consider these key takeaways when planning your approach:

- Identify primary benefits your company will gain from the BYOD model
- Identify your key stakeholders and gain their support
- Establish formal executive sponsorship
- Create formal policies addressing all aspects of the BYOD program
- Use communities and self-service scenarios
- Use an EMM solution like SAP Afaria to ensure that all your requirements are addressed
- Implement country by country and reuse documentation to adjust to each country's individual needs

For more information and resources on the BYOD model, please visit fm.sap.com/byod.

A BYOD program is often considered good PR for the IT team and is generally perceived as a benefit by the employees. It is important that your communication be rolled out regionally via your executive team.

Appendix: BYOD Implementation at SAP – Case Study

With more than 40,000 mobile devices in use, SAP has realized significant business benefits from getting employees mobile around the globe. The company's early and aggressive adoption of new technologies and its concrete enterprise mobility strategy have been critical to this success.

One aspect of this strategy is the company's adoption of a BYOD strategy. Driven by the consumerization of IT and the company's mobile-solution focus, SAP has developed an entire mobile platform engaging employees with applications that enable them to be more productive anywhere. In a rapidly expanding list of countries, SAP offers the option to use either a corporate-owned or personally owned mobile device for work. Employees can either purchase their device through a corporate catalogue or bring in their own device (from an approved list). This BYOD approach was put in place to address the trend of the consumerization of IT – allowing employees to own a single device for both business and personal use. The BYOD strategy enables added flexibility without additional costs and in some cases may even reduce costs for SAP.

The adoption of the BYOD model at SAP required the alignment of several key stakeholders. The program is driven and managed by IT and requires a cross-discipline team with contributions from legal, human resources, finance, IT, and internal communications departments. The team collaborated to address country-specific regulations and privacy laws, reimbursement-package negotiation between business and employees, tax considerations, and technical considerations including managing devices.

MANAGEMENT AND SECURITY AT SAP

SAP IT relies on the SAP® Afaria® mobile device management solution to manage and secure its BYOD implementation. The IT team has recognized significant benefits including:

- **100% self-service enrollment**
- Only **one minute** to decommission a device
- **92% reduction** in provisioning and app-deployment cycle times

AN INTERVIEW WITH MICHAEL GOLZ, CIO, SAP AMERICAS

A detailed video interview with Michael Golz, SAP CIO of the Americas, can be found at fm.sap.com/BYOD.

Q: What is the status of SAP's enterprise support of the BYOD model?

A: We have rolled out BYOD to several countries including the United States, Canada, Japan, Singapore, Australia, and New Zealand. We are continually adding new countries to the list and expanding our footprint of personally owned devices.

Q: How do you decide which devices make the approved list?

A: The supported device list is constantly under review as new devices come to market. Our goal is to support the devices that employees want – while ensuring that they are enterprise ready. We currently support iPhone 3GS, 4, 4S, iPad, iPad 2, the Samsung Galaxy S2 smartphone, and the Samsung Galaxy 10" tablet. New devices are tested and approved as soon as they are made available. Android devices are tested when they meet data encryption and EMM minimums.

Q: Do you allow employees to download any apps including games?

A: We do not restrict what employees can access on a personal device. If a security concern arises, we can remove e-mail and VPN access until the application is removed.

Q: How do you deal with appropriate use of a personal device?

A: All employees sign a code of conduct and a BYOD consent form.

Q: What is your standard security-policy password requirement?

A: Passwords have a seven-character minimum. We follow Fraunhofer Institute standards.

Q: Do you provide publicly available apps from app stores?

A: We provide connectivity apps like iPass, Citrix, or SAP public apps from iTunes. All other internal apps available are published on our internal app store via SAP Afaria. These apps can be accessed based on job role.

Q: Do you have applications that require single sign-on between apps?

A: We have an internal IT-built wizard to export single sign-on via a desktop e-mail client. The user can import to iOS devices via a custom app that lets other apps look in keychain for single sign-on to successfully validate the user certificate.

www.sap.com/contactsap

SAP

The Best-Run Businesses Run SAP™