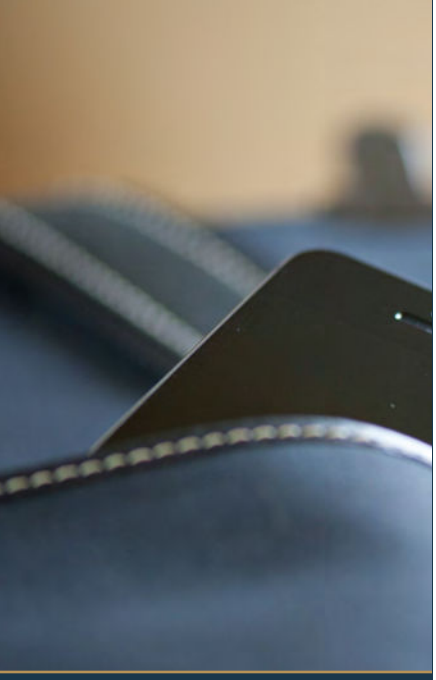
BYOD
Best Practices

Whether you have an official Bring Your Own Device (BYOD) policy in place or not, your employees are probably already bringing their own devices into your workplace—and not just smartphones and tablets. In this guide, you'll learn six best practices for creating a BYOD program that delivers real productivity and cost-reduction benefits while minimizing risk exposure.

XANTRION
I.T. AS IT SHOULD BE



Introduction

Letting employees use their own laptops and mobile devices comes with plenty of benefits, including reduced capital costs and increased productivity. That's why more and more employers who might once have resisted BYOD are now allowing it—some grudgingly, others with such enthusiasm that Gartner predicts many companies will make it mandatory.

On the other hand, BYOD also creates some significant challenges. Some of them are matters for your legal advisor, such as whether you have the right to seize an employee's device for discovery purposes or how much you're liable if you break your employee's expensive electronics. But the most pressing concerns involve IT—how to manage, secure, and support a growing multiplicity of devices, operating systems, and apps. For example:

How can IT effectively manage and support devices owned and self-configured by employees and contractors?

How do you secure employee-owned devices to protect corporate data and applications from malware and unauthorized intrusion?

How do you provide these employees and contractors with secure access to corporate networks, applications, and data on their own devices?

What is the most effective way to separate personal and enterprise applications and data on the same device?

If you haven't already set up a strategy for managing BYOD in your workplace, you're already behind the trend—and you're leaving critical issues to chance. In this guide, you'll learn six best practices for creating a BYOD program that delivers real productivity and cost reduction benefits while minimizing risk exposure.

Gartner predicts that by 2017, half of all employers will require their employees to supply their own computing devices.

Changing Expectations about BYOD

Gartner predicts that by 2017, half of all employers will require their employees to supply their own computing devices. This represents a huge shift in attitudes towards BYOD, for several reasons:

- Millennials are flooding into the workplace, bringing with them an expectation of always-on connectivity and portability. They loathe the idea of being tied to a desktop, and the prospect of disconnecting from their own devices during the work day is practically unthinkable.
- Letting employees use their own smartphones, tablets, laptops, and even desktop computers is, putting it bluntly, a source of potential cost savings in an era of tight budgets. From large enterprises that rely heavily on contractors to nonprofits and SMBs, businesses see BYOD as a way to reduce not just the up-front costs of providing and configuring mobile devices, but the ongoing costs of maintaining them.

Mitigating the Risks

Security concerns continue to be the top barrier for BYOD policies and programs. Unmanaged and untrusted personal devices create new sources of risk for IT systems and data – especially when BYOD includes notebooks and tablets.

Personal devices are especially vulnerable to data breaches. Smartphones and tablets are easily lost or stolen, potentially exposing the data stored on them. In addition, when these devices store and access data in the cloud, carelessness about security leaves that data open to being duplicated to other applications or shared to other devices. Unmanaged personal devices also risk introducing malware or other security breaches to the internal company network. To address all of these issues, companies need a BYOD program that combines policies, technology, and processes to cover all these questions:

Which users are allowed?

Using what devices?

On which networks?

To access what data and applications?

Best Practices in Six Steps

The six steps outlined below describe best practices for creating and implementing a secure BYOD program.

Establish Clear Policies and Expectations

A BYOD policy is only as effective as the employees who comply with it. You must create and share your BYOD policies and set expectations appropriately. Your policy should cover at least the following:

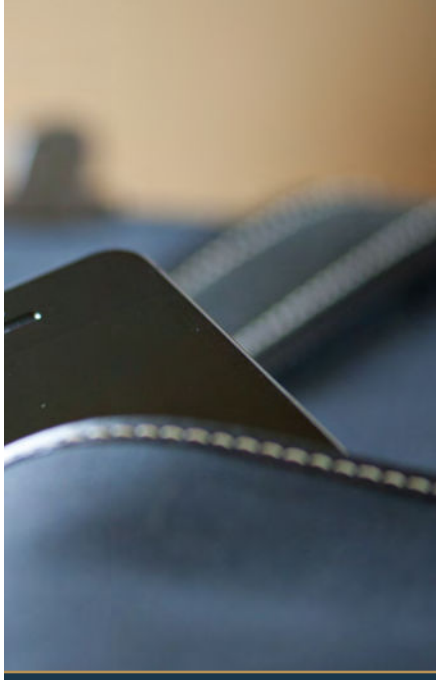
Device Options	What devices are permitted? What platforms are supported?
Participation	Who is allowed or required to join the program? Will it be restricted to certain types of employees and contractors? Are there access restrictions based on title or role?
Reimbursement	Who pays for the devices and/or for mobile data plans? While company reimbursements have been common in the past, they are decreasing as personal mobile devices become more common.
Terms of Usage	Make sure people understand what software they can run, the necessity to lock devices and encrypt data, and any monitoring and management capabilities the business may have. Many companies have employees sign a BYOD agreement to demonstrate that they understand and agree to the policy's terms.
Cancellation	Clarify what happens to any personal data within company applications and data on the personal device when someone leaves the company.
eDiscovery and Forensics	If the data on the device will ever be subject to eDiscovery, describe what will have to happen—what is the company's policy requesting physical access to personal devices?
Support	Who will support the device? Can the users turn to IT if they're using corporate applications on a personal device? Make sure support policies are clearly outlined.

Create a Separate, Secure Workspace

To control business data on employee-owned devices, IT organizations are increasingly turning to technology that lets them create a secure "container" that segregates business from personal data. One of the best ways to approach this is through virtual desktop technology that delivers access to critical data and applications without allowing them to reside on the computer or device. On laptops and desktops, the virtual desktop is essentially invisible. On mobile devices, users launch a virtual desktop app to access key documents, websites, and other applications. Anything within the virtual desktop is centrally managed by the employer's IT team, although it may continue to operate even offline. Personal data remains outside the virtual desktop, where the employer's IT team can't access it but the end user can.

Virtual desktop solutions work across a wide range of personal computing devices, from phone and tablet to desktop and laptop. These secure solutions have significant benefits for BYOD environments:

- The employer can set and enforce policies on work data and applications without affecting the user's personal computing devices or applications.
- If a device is lost or stolen, the company is not at risk since no business information resides on the device.



IT organizations are turning to technology that lets them create a secure "container" that segregates business from personal data.

The virtual desktop approach makes it easy to enforce specific access policies for individuals.

- For the user, virtual desktop solutions offer a clear separation of personal and work data and applications, thereby ensuring an acceptable level of privacy.
- Policies may be set to disallow printing, cutting and pasting, USB file transfers in the case of laptops or Windows based tablets, or other common sources of data leakage.
- Rather than managing multiple physical devices, the IT team only needs to manage the virtual desktop from a single central location.
- The centralized management console lets the IT team set and manage policies for each user across all his or her devices based on a single user profile, rather than trying to manage each device individually.

Protect Your Network

Segment and secure your network to match your BYOD strategy. Many companies maintain segregated networks for corporate and guest use. Employees using personal computing devices should be restricted to the guest network, using a secure virtual desktop on their devices to access business applications and/or company data. This protects the corporate network against a compromised employee-owned device.

Enforce Reasonable Password Policies

Authentication is another critical part of the BYOD policy. The virtual desktop approach makes it easy to enforce specific access policies for individuals. For extra security, you can require users accessing company data from a personal device to use two-factor authentication to log in to the virtual desktop. Two-factor authentication involves both a password and a secondary form of identification, such as a random number generated by the network and sent to the user via text message.

Beware, though, of making authentication policies so complex that they actually interfere with security. When you ask people to change their passwords too frequently or require 16-character passwords that are cumbersome to type on a tiny smartphone keyboard, you risk driving people to less secure behaviors—like writing down their passwords.

Address Compliance and Risk Management Mandates

To address requirements for regulatory compliance and risk management, you need full control over business data. This includes the ability to wipe company information from an employee-owned device if that device is lost or stolen, or when the employee leaves the company.

While many companies ask employees to sign agreements stipulating that the company has the right to wipe corporate data from personal devices or even wipe the device's memory completely, employees are understandably reluctant to risk giving employers unlimited access to their personally owned devices. A better strategy is to use a virtual desktop to segregate enterprise data and applications and manage or restrict access to them remotely.

Start with a Pilot Group

When you're ready to roll out your BYOD initiative, test it with a limited group within the company. Working with a small group gives you the opportunity to sort out any legal, application, security and user adoption issues that arise, ensuring a smoother rollout to the larger population.

Once you have run the pilot and worked out any issues, you can introduce BYOD policies and technologies to other groups of employees, tweaking them to address each group's unique requirements.

Putting Best Practices into Action

Xantrion provides the expertise and manpower necessary to develop and implement a sound BYOD program. We can do everything from recommending the appropriate technology approach to implementing it. Since we have successfully implemented a BYOD program for ourselves and multiple clients, we know the pros and cons of various approaches as well as implementation pitfalls. We can also provide the additional manpower required for special projects.

XANTRION
I.T. AS IT SHOULD BE

Xantrion
651 20th Street
Oakland, CA 94612

xantrion.com

866-926-8746