Best Practices to Make BYOD, CYOD and COPE Simple and Secure

Mobile productivity for your business. Freedom of choice for employees. Full security and control for IT.

Define the right bring-your-own-device (BYOD), choose-your-own-device (CYOD) and corporate-owned, personally-enabled (COPE) policies for your organization, backed by complete technologies for your digital workspace.
Employee choice has become a cornerstone of mainstream IT strategy and is essential to a digital workspace. By allowing people to choose the best devices for their needs, organizations can improve productivity and flexibility as well as job satisfaction. During the first wave of consumerization, these initiatives focused on bring-your-own device (BYOD) programs and policies. Choose-your-own-device (CYOD) soon followed, allowing users to choose a company-owned device from a small pool of company-issued devices to use for work purposes. More recently, corporate-owned, personally-enabled (COPE) programs let users to choose a company-owned device from an approved list and use their own apps as well as corporate apps on the device. While the nuances of BYOD, CYOD and COPE can vary, including their approach to cost sharing and compensation, they share most of the fundamental principles—including their security implications. Any time both personal and corporate content exists on a device, IT must ensure that effective policies and technologies are in place to protect business information—without impeding the experience or productivity of the user.

This paper provides IT executives with guidance to develop a complete strategy for BYOD, CYOD or COPE which gives people optimal freedom of choice while addressing requirements for security, simplicity and cost reduction. Based on technology foundation for a digital workspace including enterprise mobility management, desktop and app virtualization, secure file sharing and application delivery, this strategy enables your organization to:

- Empower people to choose their own devices to improve productivity, collaboration and mobility.
- Protect sensitive information from loss and theft while addressing privacy, compliance and risk management mandates.
- Reduce costs and simplify management through self-service provisioning and automated management and monitoring.
- Simplify IT with a single comprehensive solution to manage and secure data, apps and devices.

**BYOD 2.0: New models and technologies expand the options for secure employee choice**
Recognizing that employees often work best when they’re allowed to choose their own tools, BYOD policies let people use their own devices, whether occasionally, primarily or exclusively, for work. As mobility and consumerization continue to transform IT, CYOD and COPE have emerged as alternatives that combine freedom of choice with increased control for IT. COPE
can also be implemented side-by-side with CYOD or BYOD as a hybrid strategy to empower mobility in the right way for different users and groups. For example, COPE provides a way to ensure choice and mobility for employees who might not be able or willing to use their own personal devices at work, or who might otherwise be unsuitable for a BYOD or CYOD option.

The reality is that many people are already bringing their own devices to work, whether sanctioned or not. Without a coherent, comprehensive strategy for BYOD, CYOD or COPE, encompassing both policy and technology, an organization can face significant risks from security and compliance gaps to escalating IT complexity.

From a technology perspective, the most obvious question—especially where BYOD and CYOD are concerned—is how people will be able to access enterprise applications and corporate data and files on their personal devices. Simply installing apps directly on the device would raise serious security, privacy and compliance risks, license management issues and support complications, as well as restricting employee choice to Windows-based devices—and leaving other consumer devices out of the picture. For BYOD and CYOD as well as COPE, IT must also prevent the corporate apps and data on the device from being exposed to risk through the personal content it may also contain, such as when someone uses a personal, consumer-grade file sharing service to store and sync corporate data, or when a virus introduced through a personal game exposes corporate data stored on a device.

For this reason, any BYOD, CYOD or COPE program must include technologies to enable completely device-independent computing through enterprise mobility management (EMM), Windows desktop and app virtualization and secure file sharing supplemented by online collaboration and remote support services. With this approach, IT can provide optimal freedom for people while maintaining security and control. People gain single-click secure access to all of their Windows, web, SaaS and mobile apps through a unified app store on any device, over any network, with single sign-on and seamless session roaming across locations, networks and devices. IT gains a single point of control to provision and de-provision apps of all types quickly, whether to provide new resources or to cut off access when it is no longer needed or appropriate. In most scenarios, business information remains secure in the datacenter; in cases where it has to reside on the endpoint, it is protected through containerization, encryption and remote wipe mechanisms. An EMM solution that provides mobile application management (MAM) and mobile content management (MCM) capabilities in addition to mobile device management (MDM) allows IT to take a granular, app-by-app approach to security instead of or in addition to device-level controls.

In this way, IT can simplify management and reduce costs while empowering people to work easily, securely and seamlessly across any type of device, regardless of who owns the device. By leveraging the ability to granularly manage data, and application information, sensitive data can be protected while freeing IT from the need to manage someone’s personal device. IT gains identity-based provisioning and control of apps, data and devices, automatic account de-provisioning for terminated users and selective wipe of lost devices.

BYOD, CYOD and COPE policies can vary significantly from organization to organization depending on your priorities and concerns, and should be designed in consultation with HR, finance, legal and IT security teams. In general, the main differences between BYOD, CYOD and COPE deal with costs. BYOD users pay for their own devices and data plans, sometimes with a partial or full stipend provided by the company. For COPE and CYOD, the company pays directly for the device and data usage. A BYOD policy may also need to address considerations beyond the scope of COPE and CYOD, such as the question of whether employees should be paid overtime for checking email after hours or on weekends.
The following section presents guidelines and best practices for BYOD, CYOD and COPE policy development, as well as their implementation through Citrix® solutions including XenMobile®, XenApp®, Citrix Receiver®, NetScaler® Access Gateway and Citrix Workspace which includes:

**Elements of a complete strategy for BYOD, CYOD or COPE**

**Technology and systems**
- A self-service app store providing unified access and single sign-on to mobile, web, custom and Window apps on any device, over any network.
- Enterprise mobility management to secure mobile devices, applications and data.
- Secure on-demand delivery of data, apps and desktops to any device—personal or business—with tracking and monitoring to support compliance and privacy.
- Secure file sharing and sync from any device.
- Collaboration including online meetings in HD video and collaborative workspaces, available on any device.
- Remote support for people and technologies in any location.

**Policies**
- Eligibility
- Allowed devices
- Service availability
- Rollout
- Cost sharing
- Security
- Support and maintenance

**Considerations and best practices for BYOD, CYOD and COPE**

A successful BYOD, CYOD or COPE initiative combines simplicity for people with effective security, control and management for IT. While the temptation can be strong for IT to develop specific policies for every conceivable scenario, the reality is that most considerations can be addressed through the application of a few simple, consistent principles. In most cases, IT can think about how to manage and provide secure access to data and applications in terms of people, complemented with role-based management, configuration and security of personally owned and approved devices to protect the organization against threats, data loss and non-compliant usage.

**Eligibility and enrollment**

Organizations should make clear who in the organization is allowed to use personal or company-owned devices, whether on an ad hoc basis to supplement a corporate endpoint, as a permanent replacement for a corporate device or anything in between. This can be seen as a privilege to be earned, a response to employee demand, a requirement for certain types of roles, an excessive risk for some use cases or, most likely, a combination of these things.

![Figure 1: XenMobile supports enrollment for BYOD, CYOD and COPE devices](image)
Figure 2: XenMobile simplifies device enrollment. XenMobile allows IT to enroll users manually or through file import. Autodiscovery simplifies the enrollment process for users, who can use their network user names and Active Directory passwords to enroll their devices, rather than having to enter server details.

Programs that involve the replacement of a corporate device with an employee-owned device, often with a stipend provided to the employee, involve their own set of considerations. One way to determine who should be eligible for this type of program is to apply criteria such as worker type, frequency of travel, performance or whether an individual requires offline access to sensitive data. However eligibility is defined on a broad level, managers should always have final approval over which team members are appropriate candidates to receive a stipend to replace their corporate device with one of their own choosing. Managers can also be advised to apply BYOD, COPE or CYOD within the context of other departmental incentives, privileges and disciplinary measures.

Contractors are generally ideal candidates for BYOD. Many organizations already expect contractors to bring their own devices, and requiring them to do so aids independent contractor compliance.

Allowed devices

CYOD and COPE allow IT to avoid having an unmanageable diversity of devices in the enterprise environment by limiting the type of mobile devices your company will support. The granularity of this policy will depend on your user requirements, security risks and support resources; in general, the more granular your policy is in terms of device types, OS versions and model numbers, the more resources you’ll need to adequately test and support the specified devices. A more granular policy may also be more restrictive on your users—for example, by allowing only a particular iPhone model or a particular version of the Android OS.

Figure 3: Out-of-the-box device information speeds implementation. XenMobile provides a database of mobile devices to facilitate implementation. Additional devices can be added manually or through file import.
BYOD participants should be required to buy their personal devices through normal consumer channels rather than an organization's purchasing department. This helps maintain clear lines of ownership as well as ensures that participants have a direct relationship with their hardware vendor. You may want to make employee discounts available to them, if covered under your corporate vendor relationships. Some people may need or wish to supplement their device with peripheral equipment such as monitors or keyboards while at the office. In this scenario, make sure to specify who will procure and own each item.

**Rollout**

Once your BYOD, CYOD or COPE initiative has been designed, communication is vital to a successful implementation. People should receive guidance to help them decide whether to participate and how to choose the right device for their needs. They should also understand their mobile responsibilities including how data can be accessed, used and stored, and the appropriate way to set up and use work-related accounts for unmanaged consumer apps and services. Work and business data should be kept strictly segregated to support e-discovery requirements and data retention policies; similarly, work emails should never be sent from personal accounts. Acceptable use policies should apply the same way on BYO devices as they do on corporate devices.

It’s also important to provide a user adoption program to help participant get up and running. A welcome email with a link to a self-service portal can help people become more productive, more quickly.

**Cost sharing**

One of the primary benefits of BYOD is the ability to reduce costs by having people pay part or all of the cost of various devices used for work, and getting IT out of the business of procuring and supporting an expanding array of hardware throughout the enterprise. This is especially true in cases where a corporate-owned device will no longer be provided. On average, companies provide stipends in the range of 18-20 percent, though some pay more, and others offer no stipend or compensation at all. Participants should be aware that any stipend will be treated for tax purposes as income. In regions with higher personal income tax rates, you may want to increase the stipend accordingly to keep the net subsidy consistent for all participants. Any BYOD policy, with or without cost-sharing, should make clear who will pay for network access outside the corporate firewall, whether via 3G, public Wi-Fi or home broadband.

If you choose to provide a subsidy, it should reflect the full participation lifespan of each individual. Subsidies should be renewed at a regular interval to ensure that personal devices do not age beyond what would be expected for an enterprise device. If a participant leaves the company during a BYOD cycle, you may want to reclaim a portion of the current stipend.

Cost sharing has implications for the introduction of BYOD in the organization. An all-at-once rollout can increase cost as people sign up—and claim their stipends—at all points in the endpoint refresh cycle. Offering the program to people as they come to the end of their device lifecycle will spread out the impact. Organizations that do not offer a stipend can encourage full participation from day one.

**Security and Compliance**

A crucial requirement for both employee-owned and company-owned devices is to protect data without impacting user experience. For programs that allow personal apps and data on devices used for work, MAM makes it possible to keep personal and corporate apps, as well as their data, strictly separate from corporate content.
While the installation of applications directly on non-corporate devices can increase risk, a mobility program that combines enterprise mobility management, desktop virtualization and secure file sharing makes this unnecessary. All business information remains secure within the datacenter, residing on the endpoint only in isolated, encrypted form, and only when absolutely necessary. In cases where data does need to reside on the mobile device, company data can be protected through containerization, encryption and remote wipe mechanisms. To prevent exfiltration, IT can implement policies to disable printing or access to client-side storage such as local drives and USB storage.

On mobile devices, access to apps and data can be controlled, secured and managed with policies based on device ownership, status or location. IT can enroll and manage any device, detect jailbroken devices and perform a full or selective wipe of a device that is out of compliance, lost, stolen or belongs to a departed employee or contractor. Application security is ensured through secure application access via app tunnels, blacklisting, whitelisting and dynamic, context-aware policies.

![Figure 4: Mobile application management (MAM) protects company data.](image)

XenMobile provides granular app-level security controls by allowing you to add features to existing in-house and third-party mobile apps. Examples include provisioning, custom authentication requirements, per-application revocation, data containment policies, data encryption and per-application virtual private networking.

To protect the enterprise network, some organizations apply network access control (NAC) technology to authenticate people connecting to the network and check whether their devices have up-to-date antivirus software and security patches. Citrix NetScaler Access Gateway is another option for providing additional secure access capabilities. NetScaler provides granular, policy-based control including app-level single sign-on, micro-app VPN and strong passwords.

Outside the firewall, virtualization and encryption can allay most of the security vulnerabilities of Wi-Fi, WEP encryption, open wireless, 3G/4G and other consumer-grade access methods. On mobile devices, application security is ensured through secure application access via app tunnels, blacklisting, whitelisting and dynamic, context-aware policies. Network security capabilities provide visibility into and protection against internal and external mobile threats; blocking of rogue devices, unauthorized users and non-compliant apps; and integration with security information and event management (SIEM) systems.
In the event that a BYOD participant leaves the organization, the relevant policy is breached or a personally-owned device is lost or stolen, IT should have a mechanism to terminate access instantly to data and apps, including automatic de-provisioning of work-related SaaS accounts and selective wipe of lost devices. This functionality is also essential for company-owned COPE or CYOD devices, making it possible to re-allocate a corporate-owned device to a new user without the possibility that data left on the device will fall into the hands of a user who isn’t authorized to access it.

Instead of allowing open BYOD, in which people can bring any device to access enterprise apps and data, some organizations choose a managed approach. In this scenario, IT manages the personally-owned device directly, including registration, validation, authorization and device resource access.

**Monitoring and management**
For BYOD, CYOD and COPE alike, ongoing monitoring and management are essential to ensure policy compliance and determine ROI. If violations are found, IT should remind users of the relevant policy and take the actions specified therein. Some EMM solutions increase IT productivity and effectiveness by automating several aspects of monitoring and management, such as specifying the actions to be taken in response to various violations. These might include fully or selectively wiping the device, setting the device to out-of-compliance, revoking the device, or sending a notification to the user to correct an issue within a time limit—such as by removing a blacklisted app—before more severe action is taken.

![XenMobile dashboard](image)

**Figure 5:** A XenMobile dashboard provides IT with easy visibility into the mobile environment.
XenMobile helps to reduce by automating several aspects of monitoring and management. For example, IT configure XenMobile to automatically detect a blacklisted app (for example, Words with Friends). Options including specifying a trigger that sets the user’s device out of compliance when Words with Friends is detected on their device. The action then notifies them that they must remove the app to bring their device back into compliance. You can set a time limit for how long to wait for the user to comply before taking more serious action, such as selectively wiping the device.

**Device support and maintenance**

A BYOD program often reduces the total maintenance required for each device because the user is also the owner. This being said, the policy should spell out explicitly how various support and maintenance tasks will be addressed and paid for. When a personally-owned device has replaced a corporate device, there may be a higher expectation of IT support—but this should be defined narrowly to avoid exposing IT to greatly increased complexity and workload. Under most CYOD or COPE programs, IT is entirely responsible for device support and maintenance.

**A secure technology strategy for BYOD, CYOD and COPE**

Citrix enables organizations to support BYOD, CYOD and COPE through Citrix Workspace which includes Enterprise Mobility Management, Windows desktop and app virtualization secure file sharing and application delivery. In this way, IT can make enterprise apps and secure file sharing and sync available on any device people bring in to work while maintaining security and control.

Citrix solutions address all the key capabilities required to make BYOD, CYOD and COPE simple, secure and effective for any organization.

**Enterprise mobility management powered by Citrix XenMobile**

IT gains identity-based provisioning and control of apps, data and devices, automatic account de-provisioning for terminated users and selective wipe of lost devices. In addition to MDM to manage devices, XenMobile MAM and MCM functionality enables app-level security and control to protect corporate data without impacting the use of personal content on BYOD, CYOD or COPE devices.

**Windows desktop and app virtualization powered by Citrix XenDesktop and Citrix XenApp**

IT can transform Windows apps and complete desktops into on-demand services available on any device. Because apps and data are managed within the datacenter, IT maintains centralized data protection, compliance, access control and user administration as easily on personal-owned devices as on corporate-owned endpoints—within the same unified environment.

**App store powered by Citrix Receiver**

People gain the freedom to choose their own devices, including Windows and Mac® desktops and laptops, iOS, Android and Windows-based mobile products, Google Chromebooks and
BlackBerry® mobile devices—all with seamless roaming and a high-definition experience across devices, locations and networks. People have single-click access to mobile, web, data center and Windows apps from a unified app store, including integrated productivity apps with a great user experience.

Secure access powered by Citrix NetScaler Access Gateway
A unified management framework lets IT secure, control and optimize the access to apps, desktops and services on any device. Access control, auditing and reporting support compliance and data protection.

Secure file sharing powered by Citrix ShareFile
People can securely share files with anyone inside or outside their organization and sync files across all of their devices. Policy-based access control, auditing, reporting and remote device wipe help keep business content secure.

Conclusion
As a strategy at the nexus of powerful IT trends like consumerization, flexible workplaces (including telework and workplace redesign strategies), mobility and cloud computing, BYOD, CYOD and COPE will continue to transform the way people and organizations work. The right strategy, enabled through the delivery of on-demand data, apps and desktops to any device, will:

• Empower people to choose their own devices to improve productivity, collaboration and mobility.

• Protect sensitive information from loss and theft while addressing privacy, compliance and risk management mandates.

• Reduce costs and simplify management through self-service provisioning and automated management and monitoring.

• Simplify IT with a single comprehensive solution to secure data, apps and devices.

As a leader in flexible, mobile workstyles, Citrix provides complete technologies backed with proven experience and best practices to deliver successful BYOD, CYOD and COPE programs. Citrix Workspace is already helping many organizations of all sizes realize the full benefits of employee choice and mobility.

For additional information, please visit [www.citrix.com/products/citrix-workspace-suite](http://www.citrix.com/products/citrix-workspace-suite) or read our other related papers.