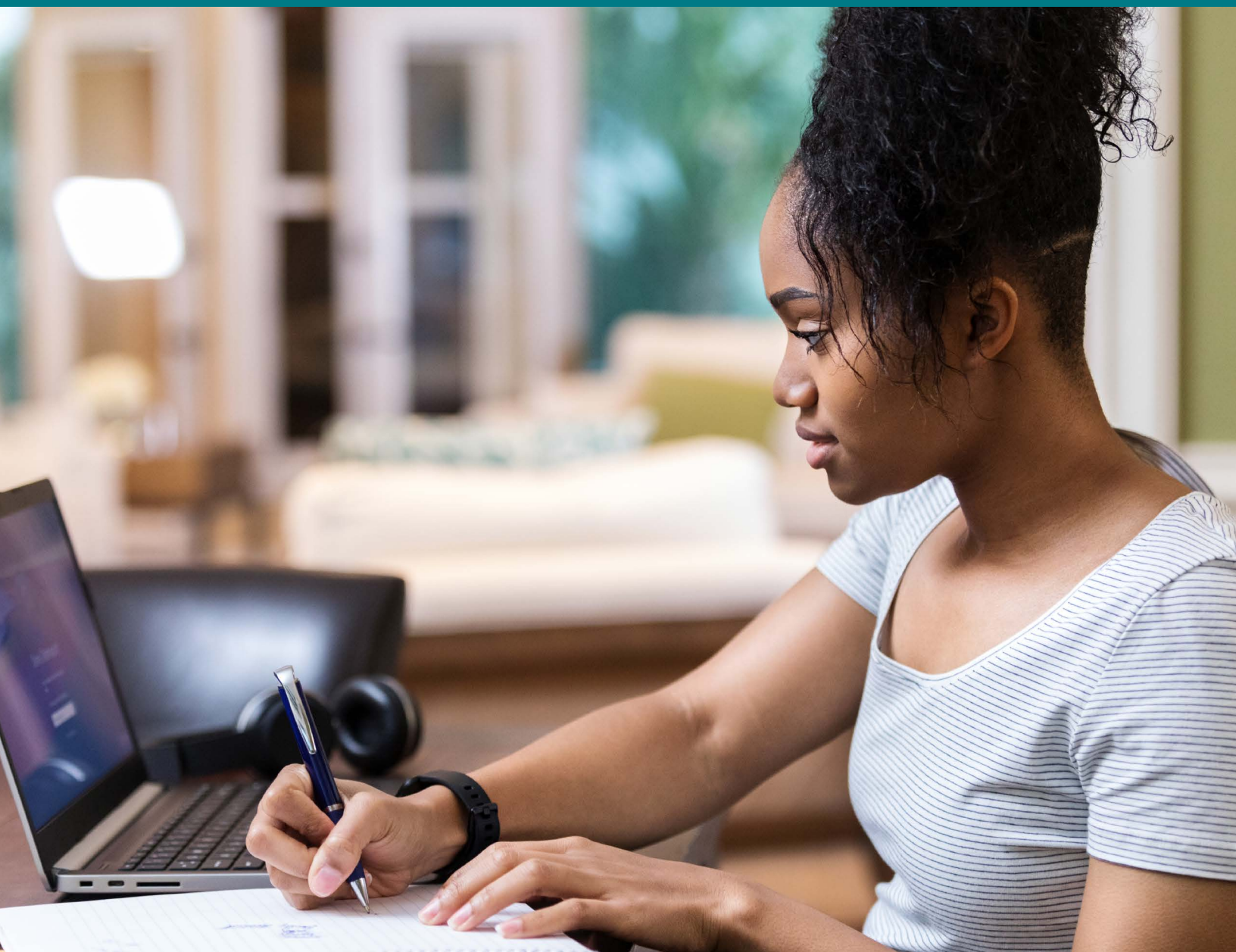
citrix

White Paper

Best practices for simple, secure device management

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



Employee choice has become a cornerstone of modern IT strategy. By allowing people to choose the best devices for their needs, organizations can improve productivity, flexibility, and even job satisfaction. With the right strategy, IT can ensure the proper policies and technologies are in place to protect business information while reducing costs and providing a great user experience.

Your strategy should enable 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.

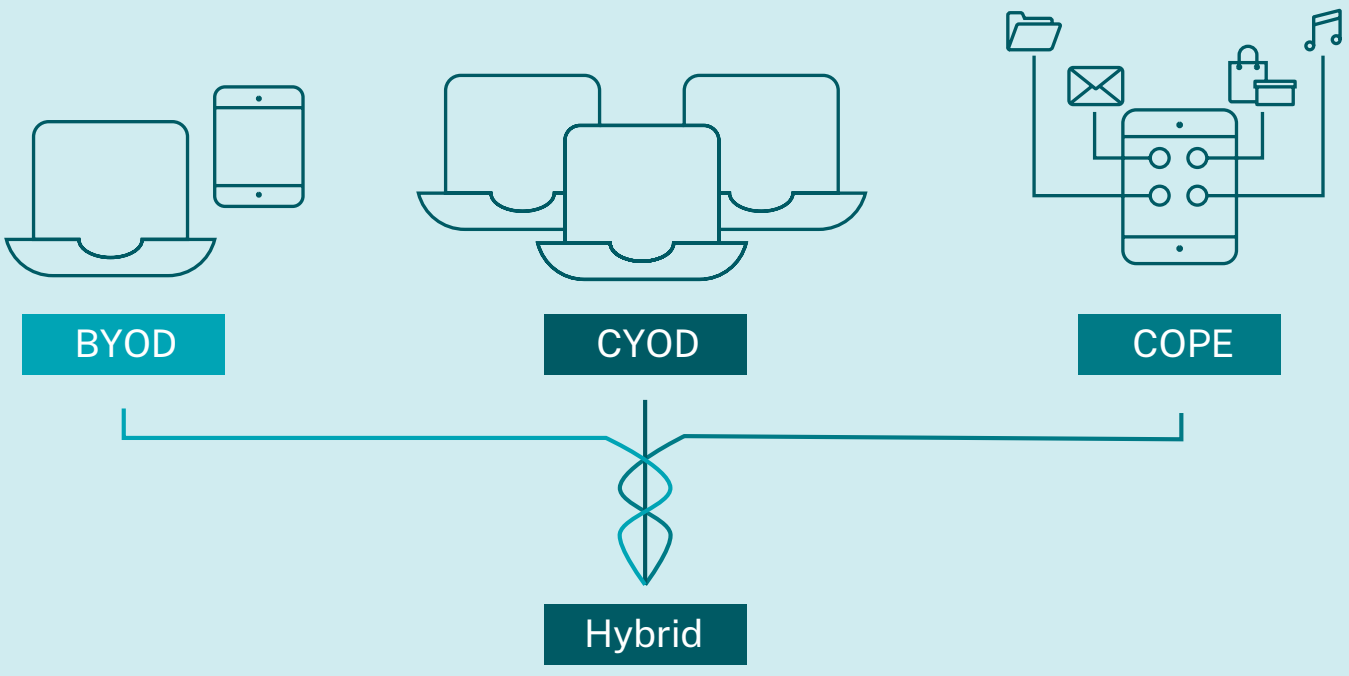
Here are 8 best practices for designing a strategy that combines simplicity for employees with effective security, control, and management for IT:

1. Choosing a policy

As mobility and consumerization continue to transform IT, there are several policies that combine freedom of choice with increased control for IT:

- Bring-your-own-device (BYOD): Lets people use personal devices for work.
- Choose-your-own-device (CYOD): Allows employees to choose a company-owned device from a small pool of devices to use for work purposes.
- Corporate-owned, personally enabled (COPE): Lets employees choose a company-owned device from an approved list and use their own apps as well as corporate apps on the device.
- Hybrid approach: A combination could be used to empower mobility in the right way for different users and groups. For example, COPE could be used side-by-side with CYOD or BYOD.

While the nuances of the policies can vary, they all share the most fundamental principles of unified endpoint management (UEM)—including their security implications. The main differences deal with cost.



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 for the device and data usage. A BYOD policy may also need to address considerations beyond the scope of COPE and CYOD, such as whether employees should be paid overtime for checking email after hours or on weekends.

2. Eligibility and enrollment

Make it clear who is allowed to use personal 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.

One way to determine eligibility is to apply criteria, such as worker type, frequency of travel, performance, or the need for 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. 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.

3. Allowed devices

To avoid having an unmanageable diversity of devices, you can limit 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.

To maintain clear lines of ownership, BYOD participants should buy their personal devices through normal consumer channels rather than an organization's purchasing department. You may want to make employee discounts available to them if covered under your corporate vendor relationships.

Some people may also want supplemental equipment, such as monitors or keyboards. Just be sure to specify who will procure and own each item.

4. Rollout

Communication is vital to a successful implementation. Provide guidance to help people decide whether to participate and how to choose the right device for their needs. They should also understand 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 participants get up and running. A welcome email with a link to a self-service portal can help people become more productive, more quickly.

5. Cost sharing

Reducing costs is one of the primary benefits of BYOD, in which people pay some or all the cost of various personal devices used for work. Companies that provide stipends typically offer in the range of 18 percent to 20 percent of the device's cost. Participants should be aware that any stipend is treated as income for tax purposes. 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.

If you choose to provide a subsidy, it should reflect the full participation lifespan of each individual. Subsidies should renew at a regular interval to ensure that personal devices don't 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 stipend.

Keep in mind that cost sharing has implications when introducing your BYOD program to 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. On the other hand, organizations that don't offer a stipend can encourage full participation from day one.

Additionally, any BYOD policy, with or without cost-sharing, should be clear on who will pay for network access outside the corporate firewall, whether via a mobile network, public Wi-Fi, or home broadband.

6. Security and compliance

A crucial requirement for both employee- 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, mobile application management (MAM) makes it possible to keep personal and corporate apps and data separate from corporate content.

Installing corporate apps on personal devices increases risk. But a strategy that combines unified endpoint management, app and desktop virtualization, and secure file sharing makes this unnecessary. Business information remains secure in your data center or cloud. And in cases when data does need to reside on the mobile device, you can protect company data through containerization, encryption, and remote-wipe mechanisms. You can also disable printing or access to client-side storage, such as local drives and USB storage.

You can control and secure access to apps and data with policies based on device ownership, status, or location. Enroll and manage any device, set passcode requirements, detect jail-broken devices, and perform a full or selective wipe of a device that's out of compliance, lost, stolen, or belongs to a departed employee or contractor. Ensure application security through secure access via app tunnels, blacklisting, whitelisting, and dynamic, context-aware policies.

To protect your network, you can apply network access control (NAC) technology, which authenticates people connecting to the network and checks whether their devices have up-to-date antivirus software and security patches.

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. 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 COPE or CYOD devices, making it possible to reallocate 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.

7. Monitoring and management

Ongoing monitoring and management are essential to ensure policy compliance and determine your return on investment.

Some UEM solutions increase IT productivity and effectiveness by automating several aspects of monitoring and management, such as specifying the actions to take 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.

8. Device support and maintenance

A BYOD program often reduces the IT 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 to avoid increased complexity and workload for IT. Under most CYOD or COPE programs, IT is entirely responsible for device support and maintenance.

How Citrix Workspace enables secure device management

Any device management program must include technologies that provide secure access to corporate apps and files on personal devices. Citrix Workspace includes all the key capabilities required to make BYOD, CYOD, and COPE simple, secure, and effective for any organization. It combines unified endpoint management, Windows desktop and app virtualization, secure file sharing, and application delivery so you can make enterprise apps and data available on any device people use for work while maintaining security and control.

Unified endpoint management

Gain identity-based provisioning and control of apps, data and devices, automatic account de-provisioning for terminated users, and selective wipe of lost devices. Citrix Workspace not only allows you to manage devices, including IoT, but it also enables app-level security and control so you can protect corporate data without impacting the use of personal content on BYOD, CYOD, or COPE devices. Citrix Workspace endpoint management allows you to choose which MAM strategy is best for you – whether that may be platform MAM such as Samsung KNOX or Appconfig, Citrix MDX (which provides an additional level of application encryption without device enrollment), or Intune MAM.

Windows desktop and app virtualization

Instead of installing and managing Windows apps and desktops on each individual device, you can deliver them as on-demand services available on any device. Because apps and data are managed within a data center or cloud, IT maintains centralized data protection, compliance, access control, and user administration as easily on personal devices as on corporate ones — within the same unified environment.

App store

Give people single-click access to mobile, web, SaaS, enterprise, and Windows apps from a unified app store. Regardless which device people choose—whether Windows or Mac computers, iOS, Android, or Windows-based mobile products, or Google Chromebooks — the user experience is the same across devices, locations, and networks.

Secure access

A unified management framework lets IT secure, control, and optimize access to apps, desktops, and services on any device, along with auditing and reporting to support compliance and data protection. Only Citrix provides unique micro-VPN to further protect application data between the mobile device and corporate resources behind the firewall.

Secure file sharing

People can securely share and collaborate on files with anyone inside or outside their organization, plus sync files across devices. Policy-based access control, auditing, reporting, and remote device wipe help keep business content secure.

With the right policies and technology in place, you can balance freedom of choice for employees with security and control for IT. Learn more about how Citrix Workspace can help you make device management simple and secure at www.citrix.com/workspace

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States