Conexlink
MyCloudIT

Increase Employee Productivity with a BYOD Policy

www.mycloudit.com

Increase Employee Productivity with a BYOD Policy

A 7-Step Checklist for MSP's and IT Departments to Implement a BYOD Policy

This e-book will give Managed Service Providers and IT departments a detailed 7-step guideline to help companies develop a good BYOD policy in place, including:

1. **Eligibility**: Who should be eligible for BYOD?
2. **Devices**: What are the minimum requirements for devices?
3. **Accessibility**: Which apps and data can your employees access?
4. **Communication:** How to explain BYOD to your employees?
5. **Costs:** What impact will a BYOD policy have on your IT budget?
6. **Security & Compliance:** How to ensure security & compliance for corporate data and applications?
7. **Support & Maintenance:** What's the new role of MSPs and IT departments with a BYOD policy in place?

Why Do We Need a BYOD Policy?

In a traditional business environment, workers suffer from productivity loss in many ways, including downtime during PC refreshes, updates, or simply when they are away from the office.

Now, as mobile devices and applications have transformed the way we live, communicate, travel, and so much more, the use of personal laptops, tablets, and smartphones for business is becoming a common practice.

There is no sense pretending that it's not happening or preventing your employees from doing so. In fact, companies are seeing a marked increase in productivity and reduction in costs by allowing employees to use their own personal devices to access company resources.

Are You Ready to Adopt BYOD?

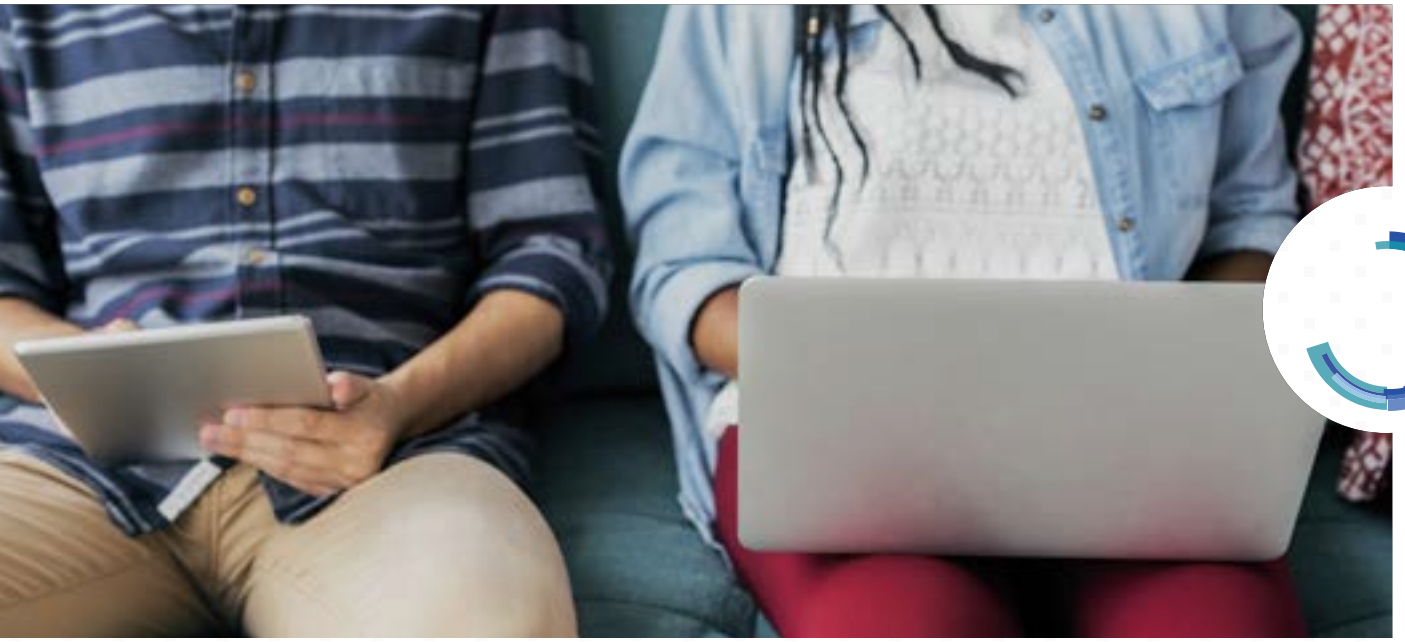
Many companies start adopting Bring-your-own-device (BYOD) policies, which allow employees to use their laptops, smartphones, or tablets for work.

This can have a very positive impact on business, such as:

- Increased productivity - enable employees to be more productive with their chosen devices;
- Greater mobility - allow them to access applications and data from anywhere, at any time;
- Lower IT budget - save resources from replacing, maintaining and updating devices regularly;

However, keeping company data secure while maintaining employee privacy is challenging for both the company and the end-users.

If you are looking to take advantage of BYOD, this e-book will help you properly set up a BYOD policy from the beginning with the following 7-step checklist!



1. Eligibility

Before announcing the BYOD policy, an organization should first determine **who are eligible to use their own devices to work**. You can take into consideration certain criteria, such as **worker type, performance or frequency of travel.**

For example, remote workers and those working in branch locations need access to apps, desktops, and data without compromising the security of the corporate network. You should enable remote or branch workers to gain remote access to everything their work requires on their personal devices.

2. Devices

If your organization wants to install applications directly on endpoints, IT will have to **determine the minimum requirements for operating system, application support, and other criteria**. This can become complicated very quickly, especially when it comes to remote support.

Instead of putting requirements on the device, **a more efficient and secure solution is cloud desktop and application hosting, which allows workers to run a full Windows desktop or certain applications on any device**. You can take advantage of the global data center network of a public cloud, such as Microsoft Azure, to ensure availability and connectivity from anywhere, at any time.

Using cloud-hosted desktops and applications helps IT focus on necessary security measures (passcode protection, anti-malware apps, encryption) rather than the devices themselves, making BYOD adoption much quicker and simpler.

3. Accessibility

A BYOD policy doesn't have to be all or nothing – you should think about **what services you want to make available on personally-owned devices and to whom. The application will vary based on user type, device type, and network**.

For example, BYOD for contingent workers should only allow access to certain applications that they would need for their contracting, consulting or freelance work. Similarly, Accounting Department and Finance Department should have access to different sets of applications and corporate data.

There are many scenarios, and you should choose the one that's best for your organization.

4. Communication

Once your BYOD policy is ready to roll out, communication will be a key to its success. Workers should receive guidance on which device is best for their needs. Corporate apps, documents, and other materials must be protected by IT if an employee decides to leave the organization, but personal emails, apps, and photos should remain untouched by corporate IT.

By setting an acceptable use policy that is signed by employees and enforced by technology, companies can avoid the possibility of legal and security issues.

BYOD policies should indicate:

- What information is sensitive
- Which security measures are mandatory
- What access locations to avoid
- Rules for sharing devices with non-employees
- Access conditions especially after employee termination

5. Costs

One of the biggest advantages to a BYOD policy is cost savings – keeping IT from spending an extensive amount of capital expenses (CAPEX) to procure and maintain certain hardware. Most importantly, **companies can transform their IT CAPEX to operational expenses (OPEX) by switching to cloud-hosted desktops and getting rid of in-house servers**.

Companies can spend these savings to offer incentives to participate in a BYOD strategy, such as rewarding employees with a stipend or some other form of compensation.

Corporate-owned Model
CAPEX

- Recycle devices every few years
- Manage & support devices
- Run on-premises servers
- Purchase warranty plans

BYOD - Cloud RDS Model
OPEX

- RDS management fee
- Cloud consumption
- Remote access licenses
- Subsidize devices (optional)

6. Security and Compliance

Most companies are concerned about the security risks involved in a BYOD policy. Installing applications directly on personal devices can raise many security and compliance concerns – this is why **an enterprise mobility management solution is recommended for a complete BYOD strategy**.

In addition, through desktop and application hosting in the cloud, **all business information remains secure within the data center – not on a worker's personally-owned device.**

With cloud-hosted desktops and applications, people gain single-click secure access to all of their Windows, web, applications, and data on any device. IT also gains a single point of control to provision and de-provision apps, whether to provide new resources or cut off access when it is no longer needed or appropriate.

7. Support and Maintenance

Because the user is also the owner, a BYOD strategy greatly reduces the total maintenance required for each laptop, tablet, or smartphone. However, **a BYOD policy must clearly define how support and maintenance tasks will be handled, and who will pay for them**.

With cloud hosting solutions, companies are only responsible for supporting and maintaining hosted desktops and applications, not the physical devices. You can increase IT productivity and effectiveness by automating several aspects of monitoring and management to scale up and down the servers based on user needs.

About MyCloudIT

MyCloudIT enables IT organizations to quickly support a BYOD policy with automated remote desktop and remote application solutions in Microsoft Azure. Visit http://mycloudit.com today to learn more!

> “You’re equipped with an automated platform that supports multiple devices – including Windows and Mac machines, thin clients, Android or iPad tablets, and smartphones.”

Conexlink MyCloudIT

Phone: +1-972-218-0715

Email: info@mycloudit.com

www.mycloudit.com