What is Bring Your Own Device (BYOD)?

Bring your own device or BYOD is a concept where employees bring their own smartphones, and computers to the workplace.

The employees use their own devices either in place of or in addition to any company-supplied devices. You may also see this concept referred to as BYOT, or bring your own technology.

More organizations are leaning toward using BYOD as more people invest in personal high-end mobile and computing devices. As more people become loyal to either Windows or Mac, and iOS or Android devices, this policy also allows employees to work with the operating system they are most comfortable with.

BYOD can sometimes happen under-the-radar. Or, it may become part of corporate policy where an organization supports the use of personal mobile devices. It’s possible that instead of supplying a company device, the company will instead provide a stipend to employees that lets them purchase a device for their use.

For instance, if an employee is client-facing, the organization may opt to provide a stipend on each paycheck that allows the employee to purchase a separate cell

phone plan or add an additional cell phone line to their service.

The History of BYOD

The concept of BYOD was first introduced in 2009 but it didn't become mainstream until 2010. As personal devices began to flood the workplace, cios began to feel pressure.

During this time, Android was starting to pick up steam and the first iPad hit the market. As a result, an increasing number of smartphones and tablets were used in the workplace and the IT department with continuing to allow employees to bring their own devices without offering a lot of support.

In response, some businesses started to block personal devices from their Network and mail servers. When iOS 4 launched in 2010, the first APIs were released to handle mobile devices. It and companies started to realize they could not ignore BYOD.

Thus, the first BYOD programs were developed in 2011 with official support introduced into the workplace. Company executives started to feel more comfortable typing on touch screen keyboards and the enterprise mobility market also began to rapidly shift.

Even though it still had to focus on securing the devices, the first real concerns around data leakage and security weren't experienced until 2012. People begin to show increased concern about their privacy.

Businesses began to focus on clearly communicating BYOD policies to those concerned users while also working toward understanding both the security and privacy implications. This caused an increased demand for Mobile Device Management (MDM) solutions.

BYOD changed the way that companies provided access to computer networks. Traditionally, the IT department would build closed networks that can only be accessed by computers the company owned. With bring-your-own-device however, employees were able to link their own smartphones, tablets, and computers to more open networks.

We can thank the wild popularity of smartphones and tablets along with the lower

cost of laptop computers for the BYOD movement. People who used to depend on the organizations to issue them hardware for work are now able to easily own personal devices that are able to perform the same work

> *Though young in the relative timeline of technology, we can expect that BYOD will become mainstream for most industries. As technology grows, security will improve.*

Benefits of BYOD

Implementing a bring-your-own-device policy in your company comes with advantages. These include:

- **Increased employee productivity:** One study showed a 16% boost in productivity over a 40-hour workweek.
- **Increased employee satisfaction:** Employees are happier with their jobs and more likely to stay with the company as a result of the flexible work arrangements.
- **Increased employee effectiveness:** Because employees are more comfortable with their own devices, they can get work done faster and more effectively.
- **Saves the IT department (and company) money, overall:** IT doesn't have to spend money on hardware, software, device maintenance, or licensing but still gets to take advantage of the upgraded technologies being integrated into the workplace.

Disadvantages of BYOD

While BYOD offers some advantages, there are also drawbacks to consider. These include:

- **A lack of network:** There's no closed, internal network, limited to just company-owned computers.
- **Accessing unsecured Wi-Fi:** Employees will undoubtedly use their devices off the clock. As such, they are likely to access unsecured Wi-Fi connections at stores, airports, coffee shops, and possibly their own homes. Unsecured networks can make it easy for hackers to access

company data.

- **Possible IT department cost increases:** If the IT department decides that they will offer support to personal devices, this could cause costs to increase a bit.
- **Lack of security on personal devices:** The employees may not have the proper antivirus or firewall software installed on their devices.
- **Possible data breaches:** Your company is at an increased risk for data breaches as a result of lost or stolen personal devices. Employees who leave the company may also put you at risk for a data breach.

BYOD Security Risks

BYOD comes with a set of security risks, outlined below.

Hardware

When a corporation provides devices to employees, the company gets complete control over the specific Hardware choice. That has been vetted to meet any corporate compliance requirements. Phones and other devices that companies provide to their employees are typically provisioned with default configurations that are capable of meeting corporate policy.

With the BYOD approach, organizations no longer control the hardware completely. They also cannot guarantee that the hardware has been vetted to meet compliance requirements.

Data Exfiltration

BYOD may also bring about data leakage or loss. If you have unmanaged BYOD devices, any users can get access to a corporate network. They will be able to take anything that they have access to and bring it with them outside the company. It’s also possible that the device could be lost or stolen, which increases the risk of data falling into the wrong hands.

Malware

An employee starts to use their own phone or computer in the workplace, not much is known about the device.

The device could be at risk from malware and other cybersecurity risks that didn't start within the company.

Since the employees also use these devices for their personal needs, company data may be at risk at any time on or off the clock. If malware was present on the device when the employee started working for the company, it could spread to other devices on the network.

This is a major issue for IT security managers.

Developing a BYOD Policy for Your Organization

An organization's IT department has to address if and how they will secure personal devices and determine the appropriate access levels. To protect your employees and your company, it is crucial to have a clearly defined BYOD security policy.

This policy needs to inform and educate employees on how to use their devices at work without compromising sensitive data.

Your BYOD policy should follow best practices. It needs to include:

- Types of approved devices – Microsoft, Apple, etc.
- Security and data ownership policies
- Whether IT support will be provided for employee's devices – and what level of support will be offered. Also, include how employees can go about getting these IT services.

An adequate BYOD program not only implements MDM to manage the devices accessing a network. It also implements network access control or NAC.

This Makes it easier to control access to corporate networks and resources. Allowing any device to connect to a company Network without control or validation won't end well.

Your policy should:

- **Specify the type of devices that will be allowed:** President Obama

used a Blackberry in the White House. These devices are incredibly outdated now but were top of the line at the time.

- **Outline a firm security policy for all devices that enter the premises:** Employees must remove lock screens and passwords from their devices so that management can access them when necessary.
- **Clearly communicate who owns what apps and data:** This way there is no confusion when an employee leaves the company. Include information about their personal data.
- **List the apps that will be allowed and what will be banned:** Some apps, though fine for personal use, present a risk to company data.
- **Set up an employee exit strategy:** What happens to the device when an employee leaves? How will management remove all access tokens, email addresses, and other proprietary information?
- **Define the steps employees should take should they get new devices while on the job**: If an employee upgrades their personal computer or smartphone, what do they need to do?

Inside this policy, you'll need to outline what you'll do to mitigate security risks as a result of BYOD. Options include:

Risk Profiling

Organizations must understand their own requirements for data protection. This is especially important in regulated industries where there are compliance requirements.

A compiled risk profile may help in determining key parts of the BYOD policy. Situations, where compliance requirements and international deployment are part of the equation, have high BYOD risk levels.

Isolating Data

Employees should never have access to more data than they need. It's always in the company's best interest to limit access to enterprise data based on job roles.

Keeping Software Up to Date

Your corporate BYOD policy should always stipulate the importance of keeping

software up to date. Employees must update operating systems, browsers, and other applications as frequently as possible.

This ensures they always have the most recent security patches. Staying up-to-date guarantees If an employee leaves the company, their devices will be adequately wiped of corporate data. If these updates aren't implemented regularly, company data could be breached well into the future.

Device Tracing

Every company should adopt a stringent device tracking policy. This ensures that they will be constantly aware of the location of all company devices when they are currently in use or not.

It's also a best practice to implement some kind of surveillance system that can monitor all the devices that are entering and exiting company premises. Any visitors' devices should also be included in the surveillance system.

Remote Wipe

Remote wipe refers to the concept of deleting data from a device remotely. This includes overwriting stored data to avoid any kind of forensic recovery and ultimately returning the device to its original factory settings.

This ensures that no one will ever be able to access the data that was once on the machine. This is particularly important to be able to do if an employee were to lose their device and not have it available to wipe clean.

If you decide to implement a BYOD policy for your company, consult with an expert to make sure you cover everything.

What's your goal today?

1. Use PLANERGY to manage purchasing and accounts payable

We've helped save billions of dollars for our clients through better spend management, process automation in purchasing and finance, and reducing

financial risks. To discover how we can help grow your business:

- Read our case studies, client success stories, and testimonials.
- Visit our “Solutions” page to see the areas of your business we can help improve to see if we’re a good fit for each other.
- Learn about us, and our long history of helping companies just like yours.

Book a Live Demo

2. Download our guide “Preparing Your AP Department For The Future”

Download a free copy of our guide to future proofing your accounts payable department. You’ll also be subscribed to our email newsletter and notified about new articles or if have something interesting to share.

download a free copy of our guide

3. Learn best practices for purchasing, finance, and more

Browse hundreds of articles, containing an amazing number of useful tools, techniques, and best practices. Many readers tell us they would have paid consultants for the advice in these articles.

Related Posts