# Bring Your Own Device (BYOD) Security Best Practices


Cybersecurity is crucial for businesses and consumers alike – with breaches in heavily regulated industries often paying fines as a result.

Smaller companies, especially those with a remote work staff may find that a bring your own device (BYOD) plan is best. When budgets are limited, it doesn't make a lot of sense to invest in equipment for staff when they likely already have laptops and smartphones that are perfectly fine to use for work purposes.

Not only can it lead to significant cost savings, but people will also generally take better care of their own devices, saving more money on repairs.

Plus, employees are often more productive and have higher job satisfaction because they are more familiar and comfortable with their own devices, allowing them to take full advantage of features.

This, along with having the freedom to choose the device rather than having one chosen for them and having to learn to use something new.

However, there are a lot of technical and legal obstacles to deal with so it is crucial to develop and enforce a BYOD policy to address any number of security risks.

For better BYOD management and security, businesses often rely on a set of written rules that their staff must agree to follow. As you develop your own corporate policy, there are certain best practices to consider.

Many of these are common across a variety of BYOD policies regardless of company size.

## Consider Device Platform and Operating Systems You'll Support

Which devices and operating systems (OS) will you support?

It's crucial to know what you require and ensure that the devices you allow support those features. For instance, if you wish to require all of your staff to lock devices with biometrics, then you can only support devices that include fingerprint readers.

You may opt to support only Apple devices or only Android devices. It all depends on your needs.

Providing company-owned devices is easier for the IT department because they can select a smaller number of devices to support.

It keeps software updates and security patch download and installation much simpler than when dealing with various devices across multiple OSs.

## Software Installed

One of the most common best practices listed in a BYOD policy is for users to have installed some kind of security software on their personal devices.

This includes antivirus software, mobile device management (MDM) software, and unified endpoint management (UEM) software.

## Maintenance Requirements

Your policy should also clearly outline the user's responsibility when it comes to device maintenance. Generally, the employee remains responsible for the

maintenance costs, though your company may choose to reimburse it.

Many organizations opt to restrict the number of third-party providers that can be used for maintenance, such as only allowing authorized dealers and resellers to perform maintenance and repair tasks. Knowing who is doing the work helps ensure mobile device security.

## No Camera or Video

Though the majority of mobile devices feature cameras, companies don't want their employees to use them while at work.

Many BYOD policies feature this restriction. There are small devices that make blocking the camera fairly easily. These can be removed when a team member is off the clock.

## Solid Passwords

Having a strong password is a must for any mobile device. All team members need to be required to maintain one. when lifting this requirement in your BYOD policy, also mention that after several failed attempts, the devices should be automatically locked until IT can reopen it.

> *Educate your staff to ensure they know what a strong password is. It is possible to create strong passwords while keeping them easy to remember, and unique for each login.*

## Other Basic Security Options

Beyond requiring employees to secure their device with a strong password, you can also request they use other security measures such as an unlock pattern, biometric authentication, and facial recognition to unlock the device.

Require the use of multi-factor authentication.

This adds an extra layer of security by requiring your employees to prove their identity before allowing passwords to be reset or accounts to be accessed from an

unfamiliar location.

## Provisioning

Before anyone can access company data and intranet on a personal device, some companies enforce a rule where IT much first provision the devices.

This ensures the apps are configured correctly and helps to enhance security.

## No Work While Driving

If anyone who works for your company is doing work-related tasks on a mobile device while they're driving and causes an accident, your company could be held liable.

To protect against that liability, you are BYOD policy should include a rule against using personal devices for work activities while driving.

## Required Data Encryption

Data encryption is one of the strongest ways to prevent hackers from getting access to sensitive information on a mobile device.

As such, it is a crucial part of securing personal devices and is a common part of any BYOD policy.

## Restrictions on Transfers of Company Data

In certain situations, employees may store company information on a personal device.

The strongest BYOD plan should prohibit staff from transferring any company-related information to an unsecured location such as a cloud-based app.

Be sure to outline expectations on how to transfer data as needed with security measures in place and which cloud-based apps are secure enough to allow for

transfer.

## No Privacy

Privacy issues are often controversial at work, especially when it comes to personal devices.

Some companies, and in an effort to protect themselves against lawsuits, dictate in their BYOD policy that employees who are using personal devices needn't have any expectation of privacy.

There are exceptions to this, but those apply only to circumstances that are governed by law.

## Reasons for Erasing Data

One of the most popular ways to protect data on mobile devices is the ability to remotely lock and wipe the device when a threat is suspected or identified.

A proper BYOD security policy should outline all of the reasons why a company may decide to wipe data. This way, employees are aware of what to expect since their personal data will also be erased.

## Right to View Employees' Mobile Records

Some companies choose to prohibit employees from using their own devices for personal calls and messages during their work shift.

Occasionally, you may find a policy that takes things a step further and grants managers the right to review employees' mobile records to see if any personal activity took place during work hours.

## Reporting Devices Lost or Stolen

Users should be required to alert the IT department if their personal device was either lost or stolen within 24 hours of the event, to allow for remote locking and erasure of the device. If desired, your policy can also require a report to be made

to their carrier, as well.

## Policy Compliance Failure

If and when an employee breaks your organization's BYOD policy, strict punishment should be enforced.

Some companies choose to remove all connectivity privileges. In some cases, it may be grounds for termination if an employee is found in violation of the policy or is otherwise non-compliant.

## When Employees Leave

When an employee leaves either because they are fired or they choose to move to another company, organizations need to have an inspection policy in place for personal devices.

This allows the IT department to request a device inspection before the employee leaves to ensure they are not taking confidential or sensitive information with them.

## Communicating BYOD Plans and Policies With Employees

All users need to be aware of the entire policy and should be required to sign an agreement before they enroll in your BYOD program. This process should be applied consistently across all BYOD devices.

If there is ever an employee who does not agree to all of the terms and conditions of your agreement, it's crucial that you do not allow them to enroll in your program.

Rather than using their personal device for work, you should either provide them with devices that are set up to your specifications and requirements.

In the event an employee who is not part of your BYOD program leaves the company, you can take possession of the company-provided material, with an

inspection process similar to the one used with personal devices.

Companies need a strong security strategy to deal with a number of security threats every day. Even something as simple as an employee leaving their computer unattended in a coffee shop while in the restroom could wreak havoc and leave sensitive data exposed.

For organizations that don't want the investment associated with company-owned devices or the full risks associated with BYOD, there is a hybrid option.

This approach allows certain employees (like those with access to the most sensitive data) to use company-owned devices for better access control, while others (the ones who lack access to confidential data) are allowed to use their personal devices with little to no increased security risk.

# 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