Are you looking for trouble?

Without a policy roadmap for bring your own device (BYOD), you're asking for it.

GFI®

BYOD Policy Roadmap

The time is now

Personal smartphones, tablets and other mobile devices certainly have their work-related advantages: At any time, from virtually anywhere, employees can access contacts and files, and an array of media, apps and tools. This certainly boosts efficiency and increases productivity.

But just as the bring-your-own-device (BYOD) initiative offers a bundle of benefits, it can also create problems. Less than one-quarter (24%) of companies have a formal BYOD policy while 36% don't plan on adopting one, according to CompTIA's second annual Trends in Enterprise Mobility. IT departments are left supporting machines the company didn't buy or configure, a scenario that potentially offsets years of hardware and software standardization efforts. As a result, administrators must manage an array of devices – all configured uniquely and lacking corporate applications, and security and management tools.

Findings by Forrester Research illustrate the tall task facing IT departments in businesses big and small. According to Mobile Is The New Face Of Engagement, researchers predict that in 2016 there will be 257 million smartphones and nearly half as many tablets (126 million). And that's in the United States alone.

It stands to reason that many of these devices will connect to corporate networks.

In today's multiplatform environments, standardization is more about IT policy than supporting specific devices. The same approach must be applied to BYOD. With the right policy, BYOD can be as safe and easy to manage as corporate-acquired computers.

Companies yet to embrace BYOD can't continue ignoring its presence much longer. Forrester says that 37% of information workers in the US today use devices without IT or corporate permission. And Gartner predicts that by 2017, 50% of employers will require employees use their own devices to do their jobs.

At this moment, there's a good chance your business supports BYOD – and you may not even know it. This is particularly true for companies whose workforces consist of young professionals.

"This new generation of workers has always used their personal devices in their school, and they have never been without these. So they see it as a step backward when they enter the workforce and get a heavy computer or antiquated smartphone," Gartner Vice President David Willis told CNBC. "Companies don't really have a choice. These young employees are going to attempt to connect devices online whether you like it or not."

Regardless of employees' ages and their level of tech-savviness, it's risky to postpone creating a policy. Without one, your company is subject to:

- Data leakage and data theft
- Malware attacks
- Hackers exploiting unauthorized devices for access
- Legal and regulatory compliance violations

As these issues relate to time, money and reputation, they can all have crippling effects on your business.

"By doing nothing, company security is at risk as employees access email and other potentially proprietary data on their mobile devices," TechRepublic Senior Editor Teena Hammond wrote for sister site ZDNet. "With a policy in place, access to data is controlled, and productivity can be extended to these devices."

Whether your company's industry is IT, legal, healthcare, manufacturing, education, finance, or something else entirely, there is a common denominator when it comes to BYOD: Your business must have the proper infrastructure in place. With that in mind, consider this eBook a blueprint for building a cost-effective BYOD policy – one that applies to businesses of all sizes and sectors.

Why wait any longer? Let's get started.

First things first

Building an effective BYOD policy is a process. It is therefore important that you take a project management approach to this undertaking. So, first things first: You need to build your BYOD team, which will, in turn, build the policy.

Adopting this approach ensures three things:

- Key decision-makers are fully involved. They may be stakeholders, executives, managers, end users, IT, legal staff, or some combination thereof.
- Necessary research and planning meetings are scheduled and held.
- A detailed BYOD policy is created, reviewed, revised and approved.

If you think this is a waste of time, think again. According to a study by global consulting firm McKinsey & Company, 50% of all large-scale IT projects fail. On average, the study found, "large IT

projects run 45% over budget and 7% over time, while delivering 56% less value than predicted."

The firm defined large projects as those that cost more than $15 million. Now, before dismissing the statistics based on the price point, look at the top reasons so many projects do not succeed:

- Lack of focus and unclear objectives (13%)
- Unrealistic schedule and reactive planning (11%)
- Shifting requirements and technical challenges (9%)
- Unaligned team and lack of skills (6%)
- Unexplained causes (6%)

You might not spend $15 million on building a BYOD policy. But it shouldn't be hard to imagine at least one of those issues, if not a combination of them, arising without the necessary personnel contributing to this project.

Start with a strategy session

Once your BYOD decision-makers have been determined, policy prep can begin.

Think of this entire process like building a pyramid. You first need to address general topics and areas that serve as the base, or foundation, for your policy. Once those areas are covered, you can add aspects to your policy that achieve a more specific purpose.

So, at this stage, your first order of business should involve completing the following action items. This exercise forces you to examine your company and its BYOD needs with a critical eye. Working through this six-step checklist will help shape the direction your BYOD policy takes:

Establish goals you want to achive

Setting goals (and prioritizing them) is a critical first step in the policymaking process. What is your primary goal? For instance, do you want stronger security? Are you interested in increasing productivity? Do you merely want employees to have more flexibility? Perhaps all of the above apply.

Consider this: According to Intel's Insights on the Current State of BYOD in the Enterprise, "Security, manageability, and remote wipe capabilities are top requirements for a successful BYOD program."

Identify existing policies

Most businesses have a range of other policies in place, including rules for security, conduct, email and confidentiality. Your BYOD policy should exist within the context of existing IT and corporate policies.

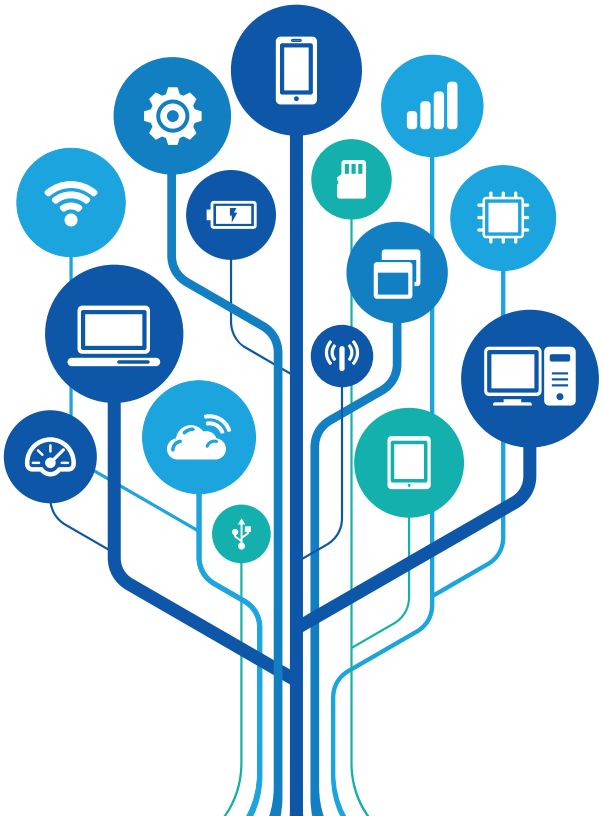
In other words, all policies should complement each other.

Therefore, it is important to determine if any of your existing policies conflict with your desire for BYOD. Some companies, for instance, already have standards for corporate-issued smartphones and mobile devices. These existing policies, as long they are current and practical, are a good starting point. Your BYOD policy should reflect that end users are in full compliance with these other policies.

Decide how to segment users

Rarely does a company's BYOD policy adopt a "one-size-fits-all" model – and with good reason. Top decision-makers like the CEO and CFO require a higher level of clearance than, say, employees such as sales associates.

How many people work in your organization? What are their responsibilities? And do you want their permissions to be the same across the board? If not, how will you group your BYOD users?



Learn whether monitoring, management and security tools are in place

Once a device is allowed on the business network, the IT staff is responsible for keeping it from causing damage. You need to know the device exists, how it is configured, and where it might be vulnerable. One area of vulnerability is remediated through proper patch management. Another area of exposure is blocked through anti-malware/antivirus software.

Once on the network, devices should be tracked through a quality remote monitoring and management tool that can spot problems before they wreak havoc.

Define scope and level of support

While end users need to know what is expected of them in terms of policy compliance, they also need to know what they can expect in terms of support. Clearly, IT has to support any corporate applications that run on the client machine. But a determination must also be made on any additional support the help desk and administrators will handle.

In that vein, your BYOD strategy must empower IT administrators to take the appropriate action when it is required.

Set boundaries

Clear expectations regarding privacy need to be defined. What employee information is considered confidential, and how is it protected? That said, can the company access, monitor and review data on employee-owned devices? Does the company retain the right to audit a personal device if an employee is no longer working for the organization?

Some businesses have employee monitoring systems. How does this apply to BYOD? Should you be able to enforce acceptable use policies by reading personal text and email messages, monitoring content and tracking browsing history?

Along these lines, BYOD doesn't guarantee employees permission to use all features of their personal devices. This is particularly true in environments where security is heightened. For supremely private businesses, camera functionality, and audio and video capabilities may have to be disabled. Other items that may be blocked include peer-to-peer networking; insecure tunneling; unapproved and unsigned apps; and users' ability to modify their own security settings.

Last but not least

Selecting management and security tools should come after completing these other steps. Otherwise, you risk spending time and money on solutions that might not meet your BYOD needs.

Keep in mind: Centralized asset management, vulnerability assessment, remote monitoring and management, patch management and backup can all help make BYOD computing safe. And a good vulnerability tool enables you to conduct regular audits so you can stay safe and accommodate new machines.

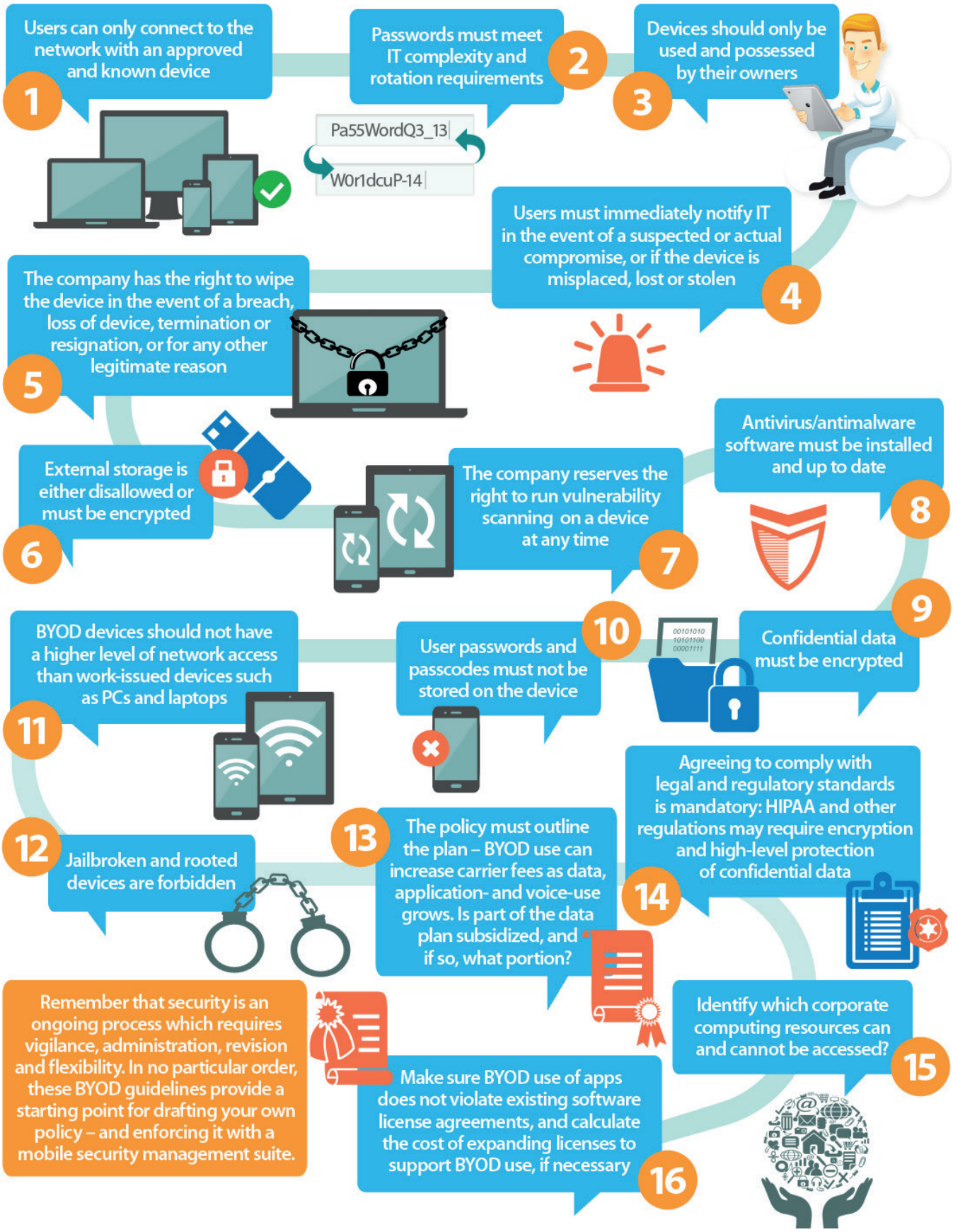
The good news about these BYOD tools is that you may have at least some of them already. And if you don't, you probably should. These tools are useful for managing your entire client device infrastructure, not just BYOD.

Policy guidelines for BYOD engagement

A step by step BYOD policy guide

Feeling comfortable with your policy prep? Then you've reached the moment of truth: It's time to build your BYOD policy. (A sample template, which we recommend you print out and reference, is included at the conclusion of this eBook.)

To make this leg of the journey easy to understand and implement, we created this 16-point infographic for quick reference. It is followed by a more detailed look at 10 key items, some of which are noted in the infographic:



Do not allow jailbroken, rooted and unlocked devices

As How-to Geek succinctly explains, "Compared to a PC, phones and tablets are fairly locked-down devices. Jailbreaking, rooting and unlocking are all ways of bypassing their limitations, and doing things that manufacturers and carriers don't want you to do."

Most, if not all, mobile security suites consider these devices "security compromised." The modifications made expose them to security vulnerabilities, malware, viruses and hacks.

Make screen lock password protection mandatory

Screen lock passwords are simple to set up, and they provide a high level of protection against data theft. Yet this basic security measure is neglected by many mobile users.

Recent findings by Consumer Reports revealed that only 36 percent of smartphone users set their screen lock with a four-digit personal identification number (PIN). Just 11% use a lengthier PIN, a password, or other unlock pattern. Meanwhile, 34% do not take any security precautions.

Write your policy to include this powerful deterrent. Mobile security suites can enforce the use of a screen lock password on any user device.

Require enrollment in the corporate mobile security management suite

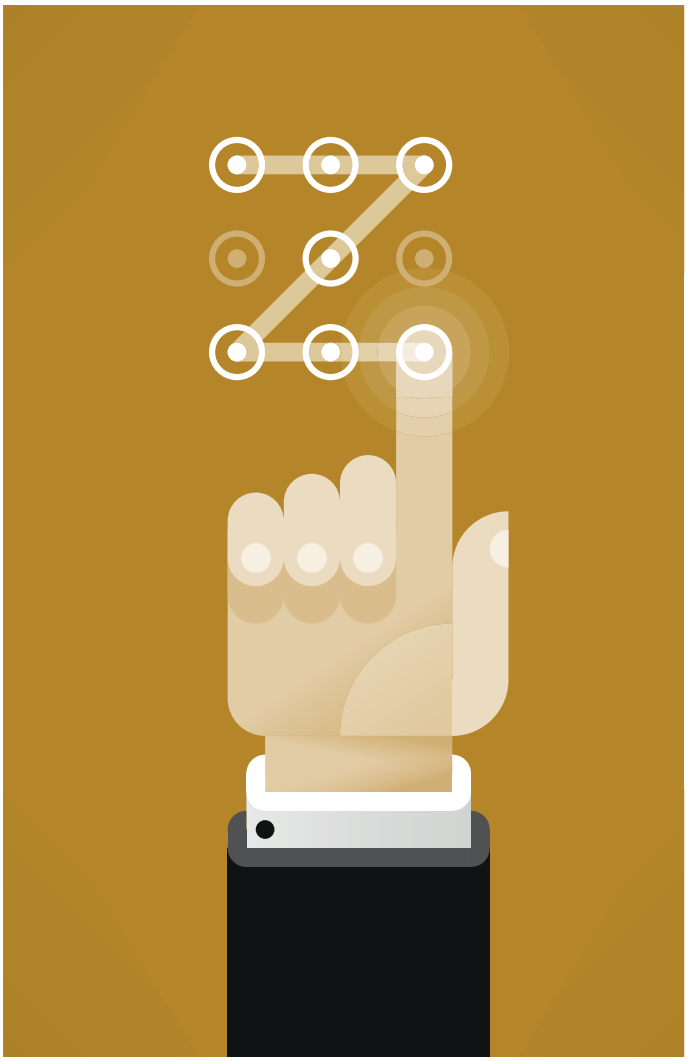
Enforcing security policies at the device, application or document level demands you use a mobile security management suite. The suite should integrate into your environment so that no user device can access corporate assets without first enrolling in and being vetted by the security policies.

Bypassing enrollment places your other users and their devices at risk.

Regularly update devices

To stay ahead of malware, users have to keep their devices updated with the latest operating systems and patches. This includes minor updates that may fix security vulnerabilities between major revisions.

You can enforce update policies and push updates from some mobile security management suites to ensure that users' devices maintain the highest available patch levels.



Keep business data and personal data separate

Because management suites have the capability of wiping data from devices, companies should provide a set of corporate apps that hold their own data separate from user data. This separation is achieved through good app planning and programming, and management suite policy enforcement.

Encrypt corporate data

All data contained within corporate apps or accessed by them should be encrypted. Taking this measure ensures that compromised devices don't relinquish their data in readable form. If users are allowed to access data in offline mode, app data is especially sensitive and must be encrypted to ensure security.

Of course, there is another approach, too. It still involves encryption – but only for data that a business deems most sensitive and, therefore, most valuable. This encrypted information would not be accessible via mobile devices, which are so often targets of hackers and malware.

As Unisys Chief Information Security Officer Dave Frymier told BBC News, "You can split your data into diamonds and paperclips, and the important thing is to encrypt the diamonds, and not to sweat the paperclips."

Regardless of the road you choose, one thing is for certain: Overall or selective encryption is crucial.

Customize profiles for devices and manufacturers

BYOD introduces a variety of smartphones, tablets and laptops – made by multiple manufacturers – into your workplace. A separate security should be available for each supported device (and it should be specific to that device).

The danger with generic security policies is they will leave significant gaps in protection and create additional vulnerabilities on your network. Most mobile management suites support a variety of device types and manufacturers. Devices outside of the support matrix should not be allowed as part of your BYOD program.

Use a VPN for connectivity

To ensure that all remote communications with the corporate network are secure, virtual private network (VPN) connection enforcement should be standard. Device-level VPNs securely connect the entire device to the corporate VPN server. Application-level, or "micro VPN" connectivity, ensures that all application-related data transmissions are secure.

Require periodic re-authentication

Periodic re-authentication confirms whether the user is genuine. Granting unlimited access without re-authentication is a security liability for any device that is stolen or compromised during authenticated use. Management suites can enforce re-authentication after a set time period.

Prevent offline access

If you require a very high level of security for particular documents or applications, prevent any offline access to them. Do not allow documents or data to be downloaded or cached on the local device. Only allow access to sensitive information while connected to the corporate network.

Common mistakes

An equally important aspect of building your BYOD policy involves understanding the pitfalls to avoid. Here are four common mistakes made during this process:

Disabling or lacking remote wipe functionality – One drawback of unprecedented digital mobility is the threat it poses to business-critical communications if a device is lost or stolen. According to a 2013 BYOD survey by IT governance, risk and compliance firm Coalfire, one-third (33.7%) of companies had no ability to wipe data contained on mobile devices.

Assuming all apps are safe – Many apps are properly vetted before being made available for download. But that's not always the case, according to a study by RiskIQ. The online security services company found that, in the Google Play™ store, the number of malware-infected Android™ apps grew 3 ½ times between 2011 and 2013 (11,000 to 42,000).

Poor password security – Many IT administrators entrust users themselves to create secure and unique passwords. It's often a hacker's dream. Security statistics from UK communications watchdog Ofcom show that 55% of adult web users use the same password for multiple sites, and 26% use easy-to-remember information.

Failure to educate – For all the guidelines and suggestions, of course, it's worth reminding that mobile device users can't be expected to follow a policy they don't understand. Training is therefore imperative. Take employees to school, so to speak. Cover passwords and device-locking as well as how to encrypt, store and back up data.

Users, in turn, must demonstrate an understanding and acceptance of the company's policy before their devices are authorized for work purposes.

Here to stay

Building an effective BYOD policy is a fluid exercise. From time to time, the policy must be reworked, perhaps due to changes in devices, regulations, corporate priorities or emerging threats. The mobile device landscape is, after all, rapidly growing and evolving.

83%

of users feel their mobile device is more important than another "must-have" for the business professional

But BYOD is clearly here to stay. If you decide to create a policy, just make sure you stay on point. There is a lot of ground to cover, so it's critical to remain focused. But if managed and implemented correctly, BYOD is beneficial to everyone: Productivity increases, as employees work more efficiently with the personal devices they are most comfortable using. And employees themselves feel satisfied, as they are empowered to choose the mobile tools that best enable them to do their jobs.

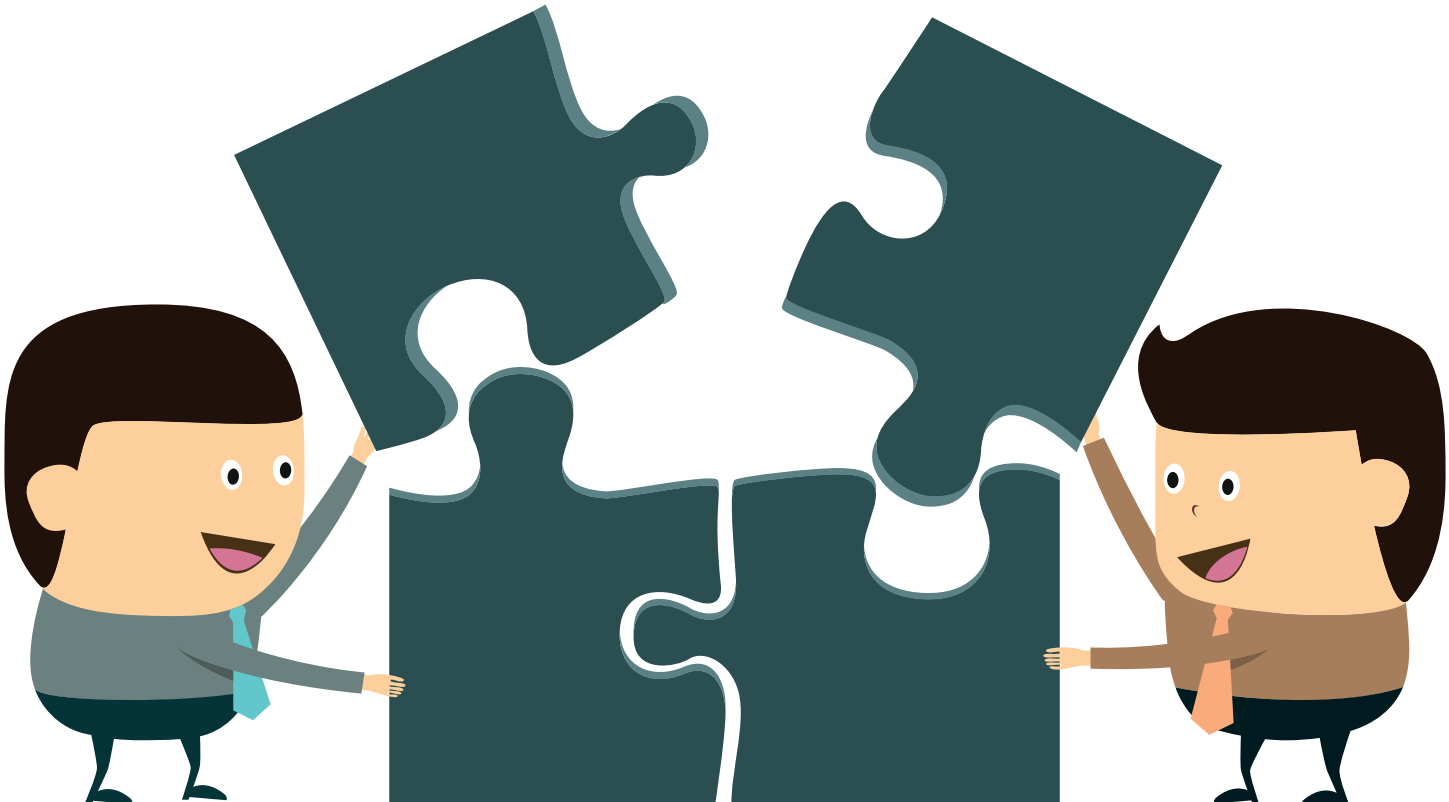
Think about this: According to IBM, 83% of users feel their mobile device is more important than another "must-have" for the business professional: the morning cup of coffee.

BYOD is going to continue building momentum. Make sure your next move is to put a policy in place.

Sample BYOD policy template

The following template, created by tech news source IT Manager Daily, is designed to help build your BYOD policy. It condenses much of the content you've read into a handy guide filled with many of the BYOD basics you should consider. Follow it point for point, or choose the items that are most important to your business.

However you choose to use it, the template has no value unless employees are well-versed in the "dos and don'ts" of BYOD. And even if employees are properly educated on acceptable BYOD practices, GFI does not guarantee the following template will result in successful implementation of your BYOD policy – nor does it accept any legal responsibility. In fact, any policy should be written with assistance from your company's legal team to ensure the language provides protection for employees and the company alike.



BYOD policy template for (your company)

(Your company) grants its employees the privilege of purchasing and using smartphones and tablets of their choosing at work for their convenience. (Your company) reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of (your company)'s data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

(Your company) employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

Acceptable use

- The company defines acceptable business use as activities that directly or indirectly support the business of (your company).

- The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.

- Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the company. Such websites include, but are not limited to: (list websites here)

- Devices' camera and/or video capabilities are/are not disabled while on-site.

- Devices may not be used at any time to:
  - Store or transmit illicit materials
  - Store or transmit proprietary information belonging to another company
  - Harass others
  - Engage in outside business activities
  - Etc.

- The following apps are allowed: (include a detailed list of apps, such as weather, productivity apps, Facebook, etc., which will be permitted)

- The following apps are not allowed: (apps not downloaded through iTunes® or Google Play™, etc.)

- Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.

- (Your company) has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

Devices and support

- Smartphones including iPhone®, Android™, BlackBerry® and Windows® phones are allowed. (The list should be as detailed as necessary, including models, operating systems, versions, etc.)

- Tablets including iPad® and Android are allowed. (The list should be as detailed as necessary, including models, operating systems, versions, etc.)

- Connectivity issues are supported by IT; employees should/should not contact the device manufacturer or their carrier for operating system or hardware-related issues.

- Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

Reimbursement

- The company will/will not reimburse the employee for a percentage of the cost of the device (include the amount of the company's contribution); or the company will contribute (insert amount of money) toward the cost of the device.

- The company will:
  a) Pay the employee an allowance.
  b) Cover the cost of the entire phone/data plan.
  c) Pay half of the phone/data plan, etc.

- The company will/will not reimburse the employee for the following charges: roaming, plan overages, etc.

Security

- In order to prevent unauthorized access, devices must be password-protected using the features of the device and a strong password is required to access the company network.

- The company's strong password policy is: Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers and symbols. Passwords will be rotated every 90 days and the new password can't be one of 15 previous passwords.

- The device must lock itself with a password or personal identification number (PIN) if it's idle for 5 minutes.

- After five failed login attempts, the device will lock. Employees must contact IT to regain access.

- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.

- Employees are automatically prevented from downloading, installing and using any app that does not appear on the company's list of approved apps.

- Smartphones and tablets that are not on the company's list of supported devices are/are not allowed to connect to the network.

- Smartphones and tablets belonging to employees that are for personal use only are/are not allowed to connect to the network.

- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.

- The employee's device may be remotely wiped if:
  1) The device is lost.
  2) The employ ee terminates his or her employment.
  3) IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

About GFI Software™: Smartly Engineered for Greater IT

GFI Software develops easier, smarter and affordable enterprise-class IT solutions for businesses. Our solutions enable IT administrators to easily and efficiently discover, manage and secure their business networks, systems, applications and communications wherever they exist. GFI is committed to its customers worldwide to deliver the trusted expertise, right-sized and smartly engineered IT solutions with a strong focus on security excellence.

GFI is a channel-focused company with a network of thousands of partners worldwide. The company has received numerous awards and industry accolades, and is a longtime Microsoft® Gold ISV Partner.

For more information about GFI, please visit www.gfi.com.

For more SysAdmin resources, news, tips and tools, visit our blog: www.gfi.com/blog

Having a BYOD policy, or any policy for that matter, is only part of the solution. Enforcing policies is important too. Sometimes organizations need software solution to do so at a granular level. Areas likes vulnerability management and internet monitoring are good examples... even more so in a BYOD world. GFI LanGuard™ and GFI WebMonitor™ are great resources to have on any network. Learn more how these two products work here:

www.gfi.com

For a full list of GFI offices/contact details worldwide,
please visit: www.gfi.com/contact-us