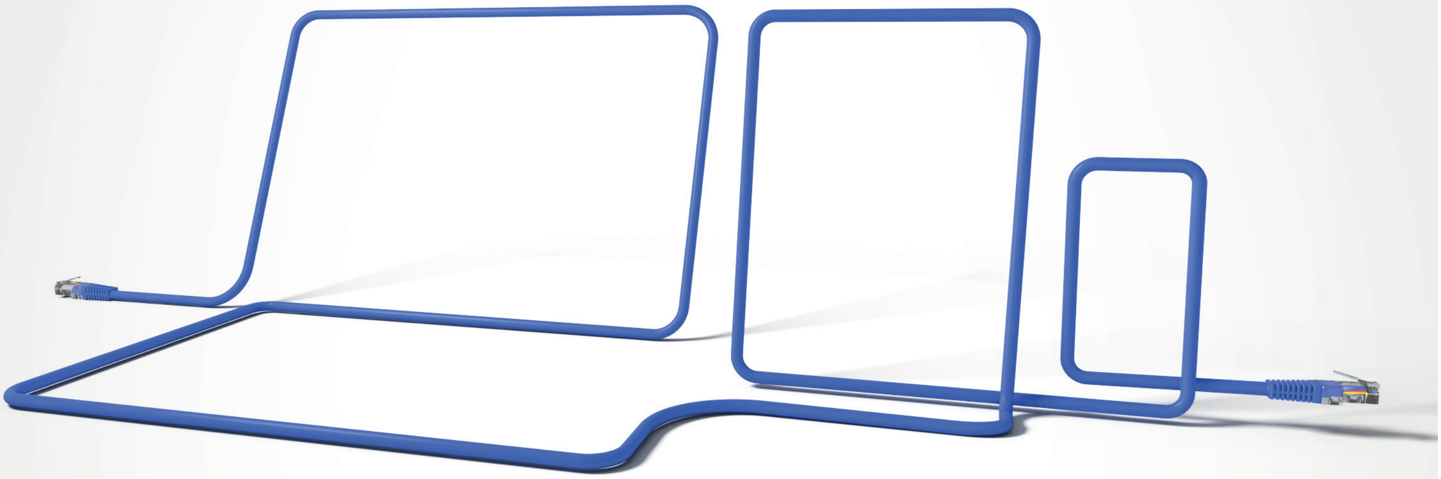


BYOD policy roadmap: Directions you can't ignore

Bring your own device (BYOD) is both an IT blessing and a curse.

GFI LanGuard™

Network security scanner and patch management

It’s great to be productive and at the same time connected to personal contacts, apps and tools, media and favorites. And happy users make for a happy IT department.

The BYOD problem

Unfortunately BYOD can bring a wealth of problems – big problems. IT is supporting machines it didn’t buy or configure. This can throw years of hardware and software standardization effort straight out the window. IT is now charged with managing an array of different devices, all configured uniquely and lacking standard corporate applications and security and management tools.

There are hundreds of millions of these devices to potentially contend with. Forrester Research, Inc. tracked the mobile and BYOD space in its “Mobile Is The New Face Of Engagement” report. Their researchers predict that in 2016 there will be 257 million smartphones and nearly half as many tablets – 126 million. All these in the U.S. alone.

> End users love to have their own devices tap into the corporate network, able to use a machine they personally picked that integrates the best of their personal and work lives.

The key mobile platforms IT will have to support are Apple® iOS, Android™ and Windows Phone®. More than 90% of mobile devices will be driven by these vendors’ technologies. You know a good portion of these devices will be finding their way onto corporate networks.

In today’s multiplatform environments, standardization is more about IT policy than supporting a narrow range of devices. That same approach must be applied to BYOD – with the right policy BYOD can be as safe and easy to manage as corporate-acquired computers.

BYOD solutions

The answer to BYOD ills is largely contained in a well-thought-out and constructed policy. You need to build a clear and detailed policy that end users understand and adhere to, and at the same time drives IT behavior and the selection of tools to manage the BYOD environment.

Actually, before you go through all the effort of crafting a BYOD policy, ask if you are willing to accept BYOD in your business in the first place. The answer should be 'yes' or 'no', never 'maybe'. Either you allow these devices to access work resources and do it properly, or you keep them entirely off the network so they do no harm (and no harm comes to them).

When contemplating BYOD, the main issues to consider are data, security, employee morale, productivity, costs, and compliance risks.

Morale is boosted by BYOD. And despite images of workers playing Angry Birds or texting friends all day, BYOD actually greatly extends the productive workday.

On the cost side, even with the need to manage these devices, BYOD is generally cheaper than buying smartphones, tablets, applications and data plans for your employees.

BYOD certainly poses risks, but the impressive benefits suggest they are well worth taking. And with a good BYOD policy and the right remote monitoring and management (RMM) tools as well as vulnerability management, and device discovery, you should have little to worry about. Even more to the point, you probably can't say no to BYOD. Forrester says that 37% of information workers in the U.S. today use devices without IT or corporate permission. You probably already have BYOD and may not even know it.

37%

of information workers in the U.S. today use devices without IT or corporate permission.

Your policy to reduce risks

Reducing risks drives much of your BYOD policy. And of course the biggest issue is security. Vulnerable BYOD devices put the entire company at risk.

Implementing BYOD costs money, but not doing it can cost far, far more.
If you have BYOD but no policy, your company is at great risk for:

Misuse of data, malware, non-work devices that are a vector for hacker access, violating compliance regulations, and a help desk swamped with unhappy users.

The BYOD policy project

Drafting a BYOD policy should be treated as a project, an approach recommended by the SANS Institute. Applying the right discipline that ensures:

- The proper stakeholders, end users, managers, executives and of course IT, are all fully involved.
- The right research and planning meetings are scheduled and held.
- A detailed document is drawn up, reviewed, revised, and finally approved.

Constructing an effective BYOD policy is an ongoing project and from time to time the policy must be reworked, perhaps due to changes in devices, regulations, corporate priorities, or threats. Mobile is, after all, a fast-moving area of technology. To help drive this process, there is a lot to be gained by becoming a student of compliance. For those users that fall under these regulations, compliance considerations will drive a great deal of your BYOD policy. Successful projects are defined by the completion of a well-structured approach. If you are just about to start on this journey, here is a 12-step program and set of considerations that can help you build a BYOD policy that will enable you to increase your productivity and efficiency while embracing the BYOD culture.

1.
What is your business all about?

Step 1. What is your business all about?

These days IT needs to be closely aligned with business objectives. And in driving BYOD policy, IT needs to define the business need for BYOD. In terms of business value from BYOD, the more mobile your workforce, the more value you will derive. If much of your workforce is fully mobile, or often mobile, it might make sense to have mobile devices be company-issued as they are a main productivity tool and should probably be specified, configured, owned and fully managed by the company. Or if not, you need a good BYOD policy.

Everyone will tell you that their security is critical. Truth be told, security is more important for some than for others. This level not only drives the rigor of your BYOD policy, but how much you need to spend on management tools. The tougher the policy, the more essential the tools. A looser aspect to your policy is having a feel for your own company. Is your business culture freewheeling, tightly controlled or somewhere in between?

2.
What do you want to achieve?

Step 2. What do you want to achieve?

Enforcing a good BYOD policy costs money both in manpower to manage and support the devices, and tools to assist IT. So what are your goals?

Productivity is clearly boosted by BYOD. Employees enjoy working on their own chosen devices. And since they have these devices with them out of office hours or while on the move, this results in extra opportunities to be productive.

Morale is another issue. Saying no to BYOD is not a morale-booster. Allowing it, however, is seen as giving workers freedom and empowerment; they will reward that freedom with a positive and productive attitude. Let’s be realistic. Many businesses develop BYOD policies to accommodate the BYOD culture that already exists. Fortunately at the same time, you’ll realize the benefits of bringing discipline to the mass of personally owned devices.

Another way a policy can help is in lowering the costs of hardware and service acquisition. That, however, needs to be balanced against understanding the upfront and ongoing costs involved in BYOD management.

3.

What policies do you have in place?

4.

Segment users

5.

Help desk capabilities

Step 3. What policies do you have in place?

Most modern businesses of decent size will have a range of other IT policies in place. Your BYOD policy should exist within the context of those existing IT and corporate policies such as security policies, codes of conduct, acceptable use policies, corporate email policies, and confidentiality agreements.

First question: Do any of these policies conflict with your desire for BYOD? Some companies already also have policies for corporate-issued smartphones and mobile devices. As these businesses transfer these machines to BYOD, these existing policies, as long they are current and well thought out, are a good starting point. Your BYOD policy should assume that end users are in full compliance with these other policies.

Step 4. Segment users

When it comes to BYOD, rare is the business where one size fits all. First issue: Do you want all users to qualify? Maybe new employees should be phased in when the level of trust increases, and you are more sure they are going to remain with the company. And low-level and temporary workers should perhaps always be denied. Once you decide who is covered, you need to determine what they can do. Not all should have the same high-level access as the CEO, COO, and other top execs.

Step 5. Examine support and help desk capabilities

If your BYOD policy does choose to accept personal devices accessing your business network, you must plan to handle to manage these devices appropriately. Even if you just agree to do tech support for the use of specific business applications, your help desk has to be able to answer employee's questions and your IT strategy must empower IT administrators to be able to take the appropriate action.

6.

Asset management principles

7.

Protection and patch management

8.

Take workers to school

9.

Level of support

Step 6. Apply asset management principles

On the infrastructure side, you'll be in good shape if you have multiplatform management tools, as well as ways to audit your network, create an inventory of existing devices and detect new ones.

Step 7. Have RMM, vulnerability assessment, malware protection, and patch management in place

Once a device is allowed onto the business network, it becomes IT's responsibility to keep it from causing damage. You need to know it 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.

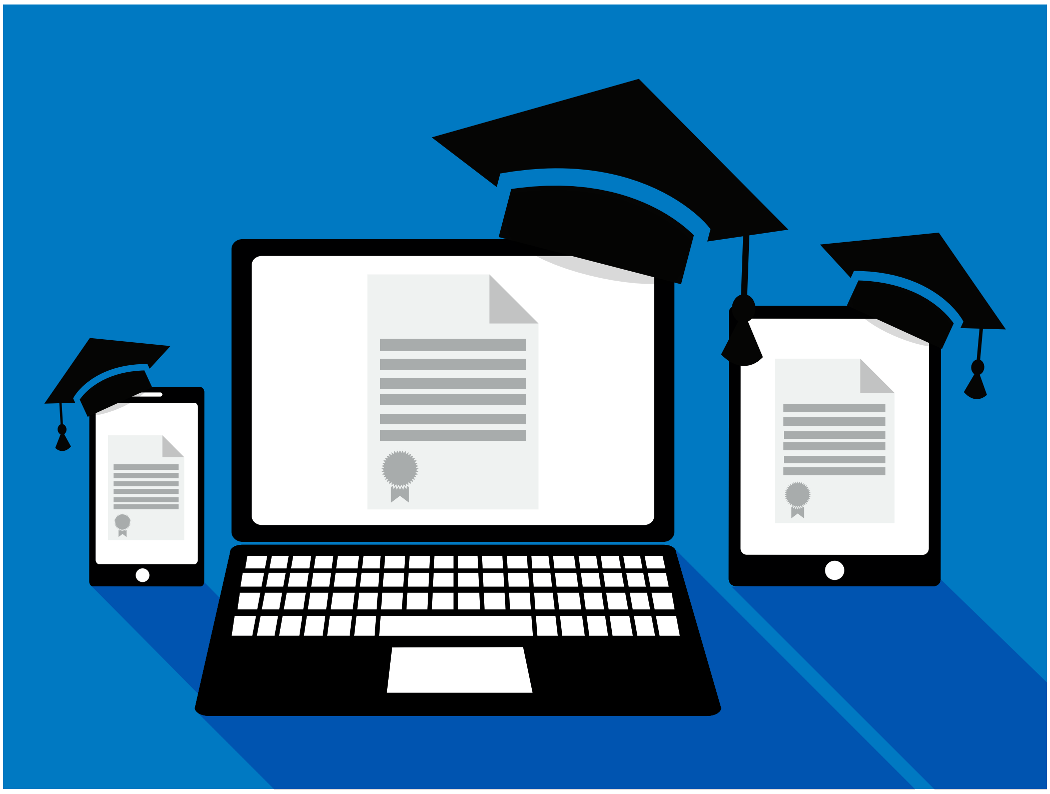
Devices should only be allowed on the network if they are known, inventoried, scanned for vulnerabilities, patched and protected. Once on the network, these devices should be tracked through a quality remote monitoring and management tool that can spot problems before they wreak havoc.

Step 8. Take workers to school

Workers can't be expected to follow a policy they don't understand. Training is imperative and should cover passwords, device-locking, how to encrypt, and how to store and back up data. Users must show understanding and acceptance of the policy before using the device.

Step 9. Define 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 apps that run on the client machine. But you also must decide what other levels of support your help desk and administrators will take on.



10.

The no-no list

11.

Privacy first

12.

Pick the right tools

Step 10. The no-no list

BYOD users must understand that they may not be able to do everything they used to do before, especially in security-sensitive environments. For super-secure businesses, camera and video and audio recording may have to be disabled if these devices aren't presently allowed in as stand-alone tools.

Other items that may be blocked include:

- Peer-to-peer networking
- Insecure tunneling
- Unapproved and unsigned applications
- Users' ability to modify their own security settings.

Step 11. Privacy first

Just as the business needs to define the rights it has to possibly access data on the BYOD device, IT also has to spell out the level of privacy BYOD users should expect. What is considered confidential for the end user, and how is this end-user information protected from prying eyes? What are your company's rights: Can you access, monitor, and review data on the device? Do you have the right to audit a personal device if an employee leaves the company? Some businesses have employee monitoring systems. How does this apply to BYOD? Can you read text and email messages, monitor content and track browsing history to enforce acceptable use policies?

Step 12. Pick the right tools

Policy should precede the selection of BYOD management and security tools. And part of that is determining what level of security you require, whether you have to adhere to compliance regulations, what exactly you want to protect and how you want to protect it.

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 lets you do 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.

16 Rules of BYOD engagement

16 rules of BYOD engagement

1. Users can only connect to the network with an approved and known device.
2. Passwords must meet IT complexity and rotation requirements.
3. Devices should only be used and possessed by their owners.
4. Users must notify IT right away in the event of a suspected or real compromise, or if the device is stolen or lost/misplaced.
5. The company has the right to wipe the device in the event of a breach, loss of device, termination or resignation, or for any other legitimate reason.
6. External storage is either disallowed or must be encrypted.
7. The device must be kept updated and patched for optimum security and the company must reserve the right to run vulnerability scanning when needed.
8. Antivirus/anti-malware software must be installed and up to date.
9. Confidential data must be encrypted.
10. User passwords and passcodes must not be stored on the device.
11. BYOD devices should have no more network access than work-issued devices such as PCs and laptops.
12. Jailbreaking is verboten. Jailbreaking phones enable users to install applications that are not released through Apple's App Store. Unofficial third-party applications could contain malicious software.
13. The policy must define who pays what. BYOD use can increase company bandwidth consumption, drive up carrier fees for data usage as data and application and voice use grows. Is part of the data plan subsidized, and if so, what portion? Should its allowance be part of the company benefits scheme?
14. You must comply with compliance. HIPAA and other regulations may require encryption and high-level protection of confidential data.
15. What corporate computing resources can and cannot be accessed?
16. Make sure BYOD use of applications does not violate existing software license agreements, and calculate the cost of expanding licenses to support BYOD use if it does.

Key policy elements

- Level and type of encryption and how this is all managed.
- The policy should define how devices are discovered to make sure all portable devices are recognized, added to an asset list, and that critical information about these devices is known and understood.
- What devices are supported? How do these devices meet your security requirements?
- What level of access will you provide?
- How are these devices secured?
- What apps are supported?
- Define how devices not covered by the BYOD policy are handled. People will still use unauthorized devices for work. And how do you block unacceptable devices?
- How is corporate and personal information handled? Who owns it, how is each protected? How is it kept separate? Who owns what?
- What are the company's rights and what are the BYOD users' rights?
- Who does the policy cover and what are the different levels?
- What devices are allowed? You must have security standards by which to judge which devices are acceptable.
- Keep it separate. Where is corporate data stored? Can you keep it off the phone and in a secure cloud or corporate server?

What next?

BYOD is an unstoppable wave. But if you decide to go with it just make sure it takes you in the right direction. Focus on the points listed above, and you'll be fine. There's no doubt that with careful thought and consideration, BYOD can boost morale, improve productivity, and will bring your company great benefits, proving to be a positive experience for all.

About GFI®

GFI Software™ develops quality IT solutions for small to mid-sized businesses with generally up to 1,000 users. GFI® offers two main technology solutions: GFI MAX™, which enables managed service providers (MSPs) to deliver superior services to their customers; and GFI Cloud™, which empowers companies with their own internal IT teams to manage and maintain their networks via the cloud. Serving an expanding customer base of more than 200,000 companies, GFI's product line also includes collaboration, network security, anti-spam, patch management, faxing, mail archiving and web monitoring. GFI is a channel-focused company with thousands of partners throughout the world. The company has received numerous awards and industry accolades, and is a longtime Microsoft® Gold ISV Partner.

More information about GFI can be found at http://www.gfi.com.

GFI 5042 oct13

GFI®

www.gfi.com

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

Other network security solutions from GFI

GFI EndPointSecurity™
Control of USB sticks, iPods and other endpoint devices

GFI EventsManager™
Log data analysis and IT management

GFI WebMonitor™
Web security, monitoring and Internet access control

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.