Contents

Introduction: The Consumerization of IT 2
BYOD Policy: An Enterprise-Wide Consideration 2
Setting BYOD Policy 3
Best Practices for Implementing a BYOD Program 8
Conclusion 15
BYOD and Good Technology’s Secure Container 15
**Introduction: The Consumerization of IT**

The consumerization of IT is coming to your business. It’s a given that employees will either bring their own smartphones and tablets into the workplace or will want to work on these devices when away from the office. Mass adoption of smartphones, tablets, and a variety of mobile applications has set expectations, causing the “I want my iPad” phenomenon to ripple through workplaces.

This trend has created new opportunities and challenges for IT managers, CIOs, and security professionals, who need to find a better way to serve internal customers with simple, easy-to-manage, secure mobility solutions. CIOs must both maintain control over corporate data security and provide a user experience that fosters happy and productive employees.

According to Forrester Research, more than half of US information workers now pay for their smartphones and monthly plans to do work for their employers, and three-quarters pick the smartphone they want, rather than accepting IT’s choice.

A Bring Your Own Device (BYOD) program comprises the corporate technology policies and procedures that provide a secure mobile computing environment on the devices employees want to use. But BYOD is not just a technology issue. It’s also a central business issue that demands an effective approach encompassing business strategy, policies, and systems.

Because employees have become accustomed to self-service environments for applications and support, thanks to innovations such as Software as a Service (SaaS), cloud computing, and, of course, mobile devices, they are also much more comfortable with the concept of a BYOD program that allows them to use their own device(s) for work. BYOD programs should reflect best practices that recognize and embrace the inevitability of consumerization, yet offer “built-in” flexibility and adaptability because those best practices are emerging and changing as quickly as the mobile environment.

**BYOD Policy: An Enterprise-Wide Consideration**

A BYOD policy should accommodate its employees’ lifestyles and work habits while protecting employees and the organization from risk. If it becomes a simple affair in the eyes of an employee to start a project at work, put it on a mobile device for the train ride home—perhaps pausing to check the news or play Angry Birds—and make final tweaks to the project after the kids are in bed, that employee will be more productive. If she can do all this on her own device, with all of her own applications intact, she will also be happier.

There are more implications.

Employees now expect that they can use business applications such as SharePoint, CRM, ERP, and custom portals on iPhones and Android phones, available from anywhere on a network.

In exchange for the freedom to use their own devices, employees are willing to accept a cost burden formerly borne by the IT department. That means IT can outsource at least some of the cost of devices, apps, and services to employees and third-party providers.

Instead of paying hundreds, even thousands of dollars a year, to purchase BlackBerry devices and data plans and provide support for those devices for the higher-level employees, the company can take any

---

number of approaches to subsidize purchases of and plan maintenance for a wider array of phones for a broader number of employees. And, by shifting routine plan and device maintenance responsibilities to employees in return for supporting the devices they want, IT can focus on more pressing issues, leading to financial benefits and less tangible, but nonetheless important operational benefits.

BYOD is new territory for many organizations, so some trepidation is understandable. BYOD affects human resources, legal, and financial departments, as well as IT, and potentially every line of business or department. When developing a BYOD program and setting BYOD policies, organizations face many challenges and risks regarding securing and managing corporate data on personally-owned devices. These challenges are highlighted in the form of questions to consider in the next section, "Setting BYOD Policy."

Only your combined HR, IT, finance, and legal teams, working together with the executive team and business unit managers, can determine the policies that best fit your organization. Your newly defined corporate BYOD policies can assist your organization in meeting financial goals and objectives and should take into consideration security, legal, regulatory, tax, and other requirements that may apply to your organization and its operations.2

### Setting BYOD Policy

As you implement a BYOD program and policy, there are four main areas to consider: general technical considerations, financial reimbursement, technical support, and liability.

#### General Technical Considerations

The organization needs to decide which platforms will be supported and how. This includes determining whether to support BlackBerry, iOS, Android, Windows, or Symbian operating systems (or some combination of those). At minimum, the organization must answer the following questions:

- What devices and mobile operating systems can we support?
- What are our security requirements at each level: devices, applications, and data access?
- What risks are we introducing by letting employees access corporate data through their personal devices? What level of tolerance do we have for those risks?
- How can we manage our mobile deployment in a BYOD world without risking sensitive data or intruding on employee’s rights to privacy on devices they own?

---

2 This guide is not intended to provide legal or financial advice. This guide does not define BYOD user policies, which may also be referred to as Individually Liable user policies. The questions and policy considerations outlined here are a set of best practices supported by several real-world examples. You should use these examples as guidelines rather than as explicit policies to adopt “as is” within your organization. This guide provides you with a framework and starting point, but your company or organization will have its own fiduciary, legal, regulatory, or other requirements that affect your BYOD program and policy needs.
Questions to Consider:

- Do we have cross-platform (iOS, Windows Mobile, and Android) knowledge, tools, and apps?
- How will we distribute applications to and manage applications on employee devices?
- How will we develop secure applications for mobile devices?
- What applications should we deploy—email, time and expense management, corporate directories, CRM?
- Will we provide intranet access to BYOD users?
- What types of users will be provided with BYOD devices? Will we provide them to everyone, or a select group that has a greater need for mobility?
- What levels of access to applications and services will be afforded to each group of users?
Technical Support

Considering the industry wide average for corporate-owned devices is $80 per month, substantial savings opportunities await organizations that switch to BYOD programs. Good Technology, a secure mobile application and device management provider, found that 77% of its customers reduced the percentage of mobile users on company-owned devices to 60% or less while 50% have been able to reduce company-owned device use to 20% or less. One of its customers, Avnet, a hardware and software distributor, was able to reduce its overall spending by 10 to 15%. Another customer, Union Bank, approximately $1 million by switching to BYOD.

When your IT department spends less time supporting devices, it will be freed up to focus on higher-value tasks. However, there are still many policy questions to consider. Here are some of the most critical.

Questions to Consider:

- What levels of support will we provide?
- Are all employees eligible for mobile access to company data and applications?
- Will we restrict access based on role, title, manager approval, geographic, or other organizational considerations?
- Will we restrict access to particular company applications or data? If so, which apps and data?
- Will we support all devices?
- What level of support will we provide for personally owned devices?
- Will we support only corporate data or apps?
- Should we support custom apps on personally owned devices?

Financial Reimbursement

From the outset, organizations need to determine how—and whether—to pay for employees’ use of mobile devices. The financial arrangement usually falls into one of three basic categories:

- Direct Billing: The organization buys the device, pays for its data plan, and all charges are billed directly.
- Stipend: The organization offers a monthly stipend to support the employee’s use of the device, typically added to a paycheck.
- Expense: The organization does not purchase phones or data plans, but each department manager can approve or reject a certain amount of employee spending on these items, reimbursing the employee based on expense reports.
Questions to Consider:

- What are the financial considerations for our BYOD policy?
- Is reimbursement available? If so, for which services (voice, data, WiFi hotspots) and under what conditions (business vs. personal usage, manager approval)?
- Are any services not eligible for reimbursement (SMS/MMS, ringtones, 411 calls, or others)?
- Are there caps on reimbursements (fixed monthly stipend or maximum expense-back limits, irrespective of charges incurred)?
- Are users eligible for full or partial reimbursement of device acquisition or replacement costs?
- Which department pays for services extended to employees on mobile devices?
- If an employee is provided with a smartphone for after-hours calls, does he receive overtime pay for taking those calls?
Managing Risk of Corporate Data Loss

Fundamentally, an IT department must develop practices that protect corporate data while maintaining employee productivity. This involves the participation and cooperation of other departments, including human resources, purchasing, legal, financial, and the lines of business that own the data. All policies about data protection need to be incorporated into the BYOD policy.

Questions to Consider:

- What are the risks for loss of corporate data or intellectual property?
- How is corporate content on employee devices managed without interfering with personal use?
- Must users sign an acceptable use policy before connecting personal devices to the corporate network?
• Is it legally acceptable to wipe corporate or personal data if the policy is violated and data is at risk of compromise?
• How much data, such as GPS data, should we collect about users?
• How should we handle lost or stolen devices?
• Will our organization enforce the use of a “whole device” password?
• Should and can we prevent jailbroken or rooted devices from accessing corporate data and apps?
• What is our policy regarding use of devices by users other than the corporate end user?
• What should happen if a user violates policy?
• Should different violations be treated differently? (e.g., eligibility vs. security vs. acceptable use)?

**Best Practices for Implementing a BYOD Program**

Leading organizations are now implementing BYOD programs to accommodate increasing employee demand for bringing and using personal mobile devices for work. Through careful consideration of the legal, financial, procedural, and HR implications, several organizations offer emerging best practices that can inform your BYOD program and policy development. Here are brief overviews of several BYOD programs.

A government research organization has been a Research in Motion (RIM) BlackBerry client since 2001 and manages 1,400 mobile devices with email functions. In 2008, the company instituted a BYOD policy for personal BlackBerries. Employees could use the RIM models and data plans of their choosing, receiving a monthly stipend to cover device and carrier costs. Over time, this organization experienced incredible demand for Apple (iOS) and Android mobile products. In August 2010, the organization expanded its BYOD program to include these devices, using Good Technology’s Good for Enterprise applications to secure and manage corporate data functions on personal devices. By 2011, 420 iOS and 280 Android devices had come online through the program, offering comparable security and superior functionality to BlackBerry.

**Best practice:** Allowing employees broader device choice while providing a stipend to cover part of their costs for using their devices for work.

A leading Blue Cross Blue Shield healthcare provider, part of a highly regulated industry with strict requirements for data control, has 14,000 employees. Several thousand employees have joined its BYOD program, which uses Good’s secure container to manage email and calendar functions on iOS and Android devices. Within 18 months, the provider practically eliminated corporate-liable devices for all but a few high-ranking executives and IT staff.

**Best practice:** Offering employees a BYOD program that allowed them to choose their own devices and supporting them with business applications led to mass adoption and cost savings.
Union Bank, also in a highly regulated industry, was an early adopter of BYOD, and now supports Android, iOS, Symbian, and RIM devices. All employees who use mobile devices for work at Union Bank do so on a BYOD basis. The IT department charges individual business departments when initiating the service. Once initiated, the program uses an “expense-back” model, in which employees submit their monthly data and voice charges to their line-of-business managers for approval. Switching to this model led to more than $1 million in annual savings.

**Best practice:** Using an “expense-back” model, which consists of setting an acceptable maximum allowable expense for employee use of mobile devices for work, and having employees submit expense reports for approval.

Fender Musical Instruments Corp., one of the music industry’s largest and most iconic manufacturers, pays directly for data plans on BlackBerries and offers a stipend for iOS, Android, and Symbian devices. The company uses Good for Enterprise to offer secure access to corporate mail, calendar, and contacts on the non-BlackBerry devices. Fender Musical Instruments estimates that the percentage of employees on the stipend program will increase from 20% to more than 50% within two years. A select few employees with highly graphical and data-intensive job requirements also direct-bill their iPhone use to the company.

**Best practice:** Writing a policy so that there are clear rules about joining, leaving or altering participation in a BYOD program.

### Examples of BYOD Programs

<table>
<thead>
<tr>
<th>ORGANIZATION</th>
<th>INDUSTRY</th>
<th>DEVICES</th>
<th>PROGRAM TYPE</th>
<th>START DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government Entity</td>
<td>Government</td>
<td>5,000</td>
<td>Expense-back</td>
<td>2010</td>
</tr>
<tr>
<td>A leading Blue Cross Blue Shield</td>
<td>Healthcare</td>
<td>5,000</td>
<td>Expense-back</td>
<td>2010</td>
</tr>
<tr>
<td>healthcare provider</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Union Bank</td>
<td>Banking</td>
<td>2,700</td>
<td>Expense-back + departmental chargeback for initiation; all devices BYOD</td>
<td>2003</td>
</tr>
<tr>
<td>Fender Musical Instruments</td>
<td>Specialty</td>
<td>440</td>
<td>Stipend for non-Blackberry BYOD</td>
<td>2010</td>
</tr>
<tr>
<td></td>
<td>Manufacturer</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Governance for BYOD Programs

**Get Executive Buy-In**

As with any technology initiative that will affect a large number of employees, executive buy-in is critical for your BYOD program.

At the outset, Fender Musical Instruments needed to obtain buy-in from the CFO, the vice president of purchasing and supply chain, and the CIO.

“It became very apparent, early on, that the only way to make this work was to have those three groups see eye-to-eye and agree about what the philosophy and policy were going to be,” says Jason Bredimus,
Fender's Vice President of Global IT Infrastructure.

At many organizations, BYOD begins not as a rank-and-file revolution, but in the executive suite. Executives get new devices such as iPads and find they deliver all kinds of useful information and programs and are easier to carry around than a laptop. They go to their CIO and demand access to corporate data and applications and expect to be supported in a way that ensures they are also secure and compliant with all business and regulatory requirements. When executives request access to corporate applications on tablets and smartphones IT has an opportunity to work directly with the executive team to set policy for the rest of the organization.

**A best practice for IT: Don’t wait to be asked.** Go to your executives with a proposal and show them how it can work and benefit the company. Find a good use case, such as using iPads for board meetings. You can supply iPads pre-loaded with the information on the meeting’s agenda, which saves paper and prevents presentations and other materials from walking out the door.

Once you’ve established executive buy-in for a BYOD program, use the opportunity to “speak as one,” clearly articulating policy so that you can avoid or dismantle any rogue departmental deployments with differing BYOD programs and policies.

**Involve Other Departments**

BYOD policies must involve other departments besides IT, particularly if the organization is paying for the phones or plans in any way. The human resources department needs to contribute and approve rules for employee conduct when using personal phones for work. Payroll needs to understand how to implement stipends or expense-back programs. Purchasing needs to understand the workflow around acquiring phones and plan policies. Line managers need to be apprised of expense procedures for employee phone use.

The IT department at a government research organization worked with HR and accounts payable to gather input for the BYOD program, policies, and processes. IT received each department’s approval before moving forward so that everyone knew their role and was in full support of the program.

Union Bank secured the approval of its security and audit departments before implementing a BYOD program that used Good for Enterprise to secure and manage data and applications on non-BlackBerry devices.

**Decide Who’s Eligible**

Most employees today are mobile employees, responding to email at lunch or at home. Nevertheless, different organizations have varying thresholds for eligibility, mostly related to cost and the regulatory burden placed on communications. Typically, the threshold is higher for organizations with a large number of employees or with significant regulatory control over their operations. In these organizations, an employee must demonstrate a need to receive email outside of corporate on-premise systems. Generally, managers must approve employees’ requests to use personal devices for work. At smaller organizations and in less regulated environments, BYOD can be offered by IT to virtually anyone with an email account and a smartphone.

**Negotiate with Carriers**

As organizations move to BYOD, their employees take on more of the cost of supporting a device and decide what devices to buy. However, mobile carriers still want the large pools of buyers they had under direct-billed bulk license agreements. The addition of smartphones and tablets means the buyer has to
purchase a data plan. Carriers offer enterprise discounts to employees for both devices and data plans. Here, a BYOD program best practice would be to get a discounted enterprise data plan for employees so that they can use their devices for work without incurring higher costs than would come with a consumer data plan.

Some organizations take certain steps to provide the best possible combination of price and service quality from their carriers. These organizations limit the number of available carriers available to users, or establish stipend and expense thresholds, making the employee liable for any costs above and beyond the discount rate.

A government research organization selected a primary carrier to support employee-owned devices and established processes for employees who wanted to migrate their work numbers to personal devices, using the organization's corporate discount with the carrier.

Prior to beginning its BYOD program, Fender Musical Instruments had a bulk discount with Verizon, but did not hold its employees to using the carrier if they chose a phone model supported by another carrier, as long as the phone’s operating system could support a secure container for its corporate applications. To maintain an atmosphere of fairness and choice, the stipend Fender pays per month for employees to use iOS and Android phones is equivalent in dollar value to the amount it pays for direct-billed use of BlackBerries.

**Technical Considerations**

**Decide on Devices**

The organizations surveyed for this report allow employees to select most iOS, Symbian and Android device types that are supported by the secure container from Good Technology. The secure container isolates employer applications from other applications on smartphones, creating a discrete environment with its own password and security controls. This allows employees to continue to use their personal smartphones and apps as normal, without putting employer data at risk. Good regularly updates its product as new devices come to market.

The device will need to meet the organization’s minimum technical standards, which should be clearly stated in the policy.

Typically, organizations will not charge employees for switching devices, if they are at the end of their contracts, but will not pay any early termination fees (ETFs) if an employee decides to switch before the end of a contract.

**Start with a Pilot**

Starting with a pilot program helps to prove the value and viability of BYOD in your organization. You can study the implications of the policy in action, alter it, and expand when appropriate. Survey and monitor participants to capture data that supports the need for a BYOD program and shows that employees prefer to use the devices they choose, and are willing (and able) to use them for work. Measure the benefits and costs—and remind your executive team that the consumerization of IT is real and demands attention. There are many articles, studies, and surveys that you can share within your organization to support the need for a BYOD program which ensures you are adequately protecting your organization’s data while permitting employees to access the information and applications they need to do their jobs.
For example, a government research organization implemented a three-month pilot program with 150 employees who were eager to use the new devices at work. The pilot was primarily intended to capture feedback about the user experience and determine which devices to support. As a result, the organization now supports most iOS and Android devices that support a secure container. In addition, the government research organization is now saving between $150,000 and $250,000 per year in hard costs to IT and shadow costs to staff and managers, who formerly had to review and approve all phone issuances and expenses.

**Automate Approvals**

To make sure your BYOD program doesn’t become a torrent of unsupervised downloads, device-switching disasters, and piles of approval forms and technical questions, establish a logical workflow. Document and communicate that workflow in the simplest terms to ensure a strong BYOD program that delivers the promised result: a more efficient, more secure, and less costly mobile communications environment.

Employees should clearly understand who in the organization is responsible for BYOD-related approvals, as well as the protocol for exception requests. Generally, the best way to limit exception requests is to require approval from a high-ranking executive, such as the CIO. Most employees will not want to bother asking for an exception if the request has to go to a C-level executive.

Automating approvals also nets benefits. By automating BYOD processes, a government research organization’s IT department kept support time and costs to a minimum, allowing them to focus on more strategic programs and projects. For example, the organization developed an online stipend request form, tied to its accounting system, which automatically routes requests to the appropriate executives for approval. The form includes checkboxes for employees to select voice, data, and device options. This approach has reduced errors, sped approvals, and reduced the time for adding new BYOD users. Renewal email messages are automatically sent to employees the month before their annual renewal period expires.

**Policies and Procedures**

**Set Stipend or “Expense Back” Policies**

Stipends are an excellent way to reimburse employees for business expenses they incur using their mobile devices. They provide a simple and consistent way of compensating employees and provide an incentive to keep excessive calling, data, or roaming charges in check. Any stipend policy should clearly state the company’s position on paying any overages, phone repair or replacement charges, or late fees incurred by the employee. The cost of acquiring a phone and fines for devices associated with accounts in poor standing are usually off the menu, but most employers at least partially fund data plans. Employees usually see this as a fair trade for being able to choose the device they want and use the additional features and apps that come with the device.

A government research organization pays employees who are approved to participate in the BYOD program a fixed monthly amount, which is included in their paychecks. The organization found the stipend model to be the easiest and most cost-effective way to manage its program. The stipend amount is based on a market analysis of the going rates for voice and data plans. Research took into account the fact that employees pay sales tax for their devices and plans and included this factor in the stipend calculation. It has three stipend levels based on voice usage ($25, $40, and $60 per month) and one stipend level for data usage ($50 per month).

Fender Musical Instruments also chose the stipend approach, after analysis showed that employees rarely exceeded their data plans’ 900-minute maximums, so it was unlikely that there would be much
need for expense processing. Additionally, the stipend approach helps people with extended plans that
include family members. Employees who are particularly vigilant about establishing an account with the
carrier of their choice can actually profit from the stipend, due to additional-line discounts offered by carri-
ers. Fender Musical Instruments still benefits in this situation, because there is no cost increase to the
company.

A leading Blue Cross Blue Shield healthcare provider wanted to maintain alignment across HR, IT, and
payroll to ensure the greatest cost efficiencies. To do so, the company uses an expense-back BYOD pol-
icy and has eliminated support for BlackBerries. Managers approve employees to receive BYOD services
and sign off on monthly expense reports. By relinquishing responsibility for the device purchase cycle, the
provider has accrued savings of approximately $25 per employee, per month, while increasing flexibility
for both the company and employees.

**Connect Policy to Process**

It is important to make sure that policy is connected to a well-defined process.

Fender Musical Instruments has a step-by-step procedure for implementing BYOD services on non-
BlackBerry devices. First, the IT department receives notification that the employee turned in his Black-
Berry. IT then emails provisioning instructions for downloading the Good for Enterprise application. Then,
the Good Technology server to notifies the IT department when an employee has actually begun receiving
mail on his own device. Lastly, the IT department notifies the purchasing and payroll departments that the
employee can begin receiving stipends.

**Decide What Support to Provide**

Most organizations we surveyed for this report were supporting corporate-liable BlackBerries before
implementing a BYOD program on employee-owned phones. From a support point of view, most orga-
nizations support the applications they authorized and deploy on the employee-owned devices. If an
employee has an issue with her device or its OS or experiences poor network coverage, the employee
must go to the vendor directly to resolve it. The enterprise has limited ability to resolve device, mobile OS,
or carrier network issues, however, if the organization detects a pattern with any particular vendor, they
can refer their employees to more reliable vendors and support only the highest-rated devices and carriers
in their BYOD programs.

Many of the organizations we surveyed save money because BYOD programs essentially get them out of
the device support obligations IT departments carry in corporate-liable programs. And because employ-
ees can choose the device(s) they want from the vendors and carriers they select, they expect less sup-
port from their employers.

As a best practice, the government research organization's IT department is available to help BYOD users
get started on their new devices. Support time is minimal, since most employees get up and running by
following the instructions in an email sent from IT. Support is then provided on an “as needed” basis. Even
so, the organization rarely has employees who encounter problems, due to Good Technology's ease of
use and reliability, combined with the thoroughly tested procedures in place.

When issues do arise, the Good Mobile Control console allows IT staff to quickly fix any problems. Good
Mobile Control provides a comprehensive mobile security and device management solution that includes
over-the-air device management, granular and consistent mobile security policy enforcement, and end-
to-end visibility for troubleshooting and support. Good Mobile Control is accessed through a web-based
console that allows IT administrators access from anywhere – including their mobile devices.
Communicate the Policy

Keeping employees informed is critical to the success of a BYOD program. Plan changes, device changes, expirations of plans, early termination fees, and policy changes must all be communicated in a clear, standardized fashion.

The IT department at the government research organization uses established communication channels, including biweekly emails, to communicate about the BYOD program. As a result, the team can anticipate questions and concerns in advance and provide specific information and directions about the BYOD program, policies, and process. They also sent email to BlackBerry users to make sure they were aware of the new devices that would become available through the BYOD program.

- Fender Musical Instruments issued a simple, four-page mobile device access policy that clearly stated:
  - The device approval process
  - A list of supported device types
  - Terms of the company’s stipend plan
  - Policy about employees paying any early termination fees for changing carriers

The policy document was accompanied by a Frequently Asked Questions (FAQ) document about the program, which the company emailed to all employees.

Fender Musical Instruments also required employees to sign a consent form that established terms of access to the corporate network. It includes a prohibition on accessing the company’s virtual private network and an agreement to accept the right of the organization to access employees’ personal devices, without notice, to investigate, delete, or wipe any company data, and disable the device for any reason. Fender’s policy states that it will not be held liable for any data loss on the employee’s phone, whether personal or corporate.

Enforce the Policy

A BYOD policy needs to have enough “teeth” to be effective. Enterprises can lose valuable data due to lack of policies, strategies and programs to support secure use of mobile devices. Organizations must have policies in place that clearly state the consequences of misuse or violation, and those policies must also provide IT with the means to act on violations quickly. It can seem like a lot for an employee to accept, but if you communicate clearly what your policies and programs are, and why they are necessary, most employees understand that it’s part of their job to keep work information secure and to comply with company policies.

The government research organization has set up enforcement policies within RIM and Good that ensures security and prevents data loss. For example, devices automatically wipe the data in the Good sandbox after the sandbox fails to connect with the Good server after a designated amount of time.

Many organizations reserve the right to wipe a device at any time—or at bare minimum, if abuse or a security breach is detected—and stipulate that they will not bear responsibility for the loss of personal data or applications if the device is wiped. Additionally, most require employees to report any loss or suspicion of compromise at the earliest opportunity. Failure to do so can result in penalties, ranging from removal from the BYOD program to termination. While these enforcement practices may sound punitive, they are necessary for most organizations to minimize the risk of data loss that could result in a breach of confidentiality or lack of compliance.
Conclusion

The proliferation of consumer devices in the workplace has created tremendous opportunity for organizations to allow their employees to work in new, more innovative and productive ways. Everyone who sets IT policy should work to accommodate and support the fact that employees are buying new devices and want to use them at work. At the same time, organizations must secure corporate data without interfering with personal use of employee-owned devices. This affects not only technology decisions, but also legal, financial, business-process, and human-resource decisions.

The old IT practice of just saying “no”—prohibiting access to corporate data from personal devices, or insisting that employees use company-owned devices for work—just doesn’t work in the consumerization era. Employees will and do find ways around untenable and restrictive policies—they have smart devices because they are smart people. BYOD is a more enlightened approach to the consumerization challenge, because it allows employees to use their own devices for work. However, BYOD works only when it is supported by robust technology and effective policies, processes and communications.

Your organization will accrue the maximum benefits of BYOD when you provide a strong and effective program for managing and supporting employee devices for work. The policies of leading organizations discussed in this guide provide a starting point for how your organization can embark on this exciting journey.
BYOD and Good Technology’s Secure Container

Good Technology offers multiple, fine-grained policy controls to provide enterprises with flexible options for setting and enforcing policies for corporate data on personal devices. Because Good separates work information in a secure container, it offers IT the security, management, and control needed to protect the enterprise. And because Good supports the most popular smartphones and tablets on the market today, it provides users with as close to native an experience as possible, while maintaining needed corporate controls.

Good’s secure container approach provides clean separation of corporate and personal data and prevents data loss or leaks to consumer apps on their smartphones and tablets. This frees employees to use the devices they want, gets IT out of the device support business, secures corporate data, and provides a less intrusive user experience. Employees can be more productive and happier with the devices they use, and the organization saves money on dedicated business devices and data plans.

In December 2009, Good Technology introduced Good for Enterprise, an enterprise mobile security platform that secures mobile devices and applications with over-the-air and on-device encryption. Good for Enterprise also includes industry-leading mobile device management capabilities via Good Mobile Control, a single web-based portal through which IT can manage all devices and remotely wipe only corporate data while leaving personal data intact. Good controls data at the application level, rather than the device level, freeing employees from having to enter a complex password just to make a call or send a text. With Good for Enterprise, IT can apply policies and prevent data loss via flexible, fine-grained controls that can easily support literally hundreds of policies at the application level, while cleanly separating corporate and personal data and applications.

Additionally, Good Technology offers Good Dynamics, which allows organizations to develop and distribute secure mobile applications or enable third-party applications, such as CRM and ERP, for employees’ use on mobile devices. As you move forward with BYOD, you can do so knowing that the same technology that supports your secure email and calendar access on mobile devices can also support applications with more robust functionality.