Planning Guide
Five Steps to Consumerization of IT in the Enterprise
Intel’s Guide to Embracing the Inevitable

Why You Should Read This Document
The purpose of this guide is to help you define an approach to consumerization that applies a user-centered strategy for supporting both employee-owned and employer-provided devices. This guide outlines five steps to help you manage consumerization in the way that works best for your organization:

- Understand the powerful—and inevitable—forces shaping consumerization today.
- Rethink user computing to optimize the compute experience and keep users productive on any device.
- Create an inclusive approach by addressing both employee-owned and employer-provided devices, and opening up a two-way channel of communication with employees.
- Support employee-owned devices with best practices that address a user-centered strategy and the inherent security issues around BYO.
- Recognize that there is no one-size-fits-all solution for consumerization: The diverse roles and responsibilities in the enterprise come with a range of technology needs.
Planning Guide
Five Steps to Consumerization of IT in the Enterprise
Intel's Guide to Embracing the Inevitable
Contents

3 A New Approach to Consumerization
4 Step 1: Understand the Powerful Forces at Work
5 Step 2: Rethink User Computing
6 Step 3: Create an Inclusive Approach
7 Step 4: Support Employee-Owned Devices
11 Step 5: Find the Right Tool for the Job
13 Embracing the Inevitable—Without Abandoning the Past
14 Resources for Learning More
A decade ago, Wi-Fi was considered a new, disruptive technology. Today, it has become the computing norm for casual and power users alike—and it continues to get faster, easier, and even more prolific. Consumerization is on a similar path. Many see it as a growing trend, but it’s the single largest disruption to client computing since Wi-Fi—and fast becoming a permanent fixture in the enterprise environment. And it’s no trend: Consumerization is here to stay.

Although definitions vary widely, many associate consumerization with “Bring Your Own”—or BYO. However, Intel has a broader definition of consumerization that extends beyond devices to include the entire computing experience: The technology we use in our personal lives—applications, hardware, and even Internet services—has a distinct impact on the technology experience we expect at work.

To address the gap in expectations—and unify the personal and professional technology experience—IT organizations must rethink their approach to managing consumerization. By driving the effort to better align the at-work technology experience with the at-home experience, you can help improve employee morale and increase productivity, all while gaining greater IT security and control. Moreover, by taking a new approach, you will have a powerful opportunity to retain your organization’s reputation as a technology innovator—especially when it comes to BYO.

### The Purpose of This Guide

The purpose of this guide is to help you define an approach to consumerization that applies a user-centered strategy for supporting both employee-owned and employer-provided devices. This guide outlines five steps to help you manage consumerization in the way that works best for your organization:

1. Understand the powerful—and inevitable—forces shaping consumerization today.
2. Rethink user computing to optimize the compute experience and keep users productive on any device.
3. Create an inclusive approach by addressing both employee-owned and employer-provided devices, and opening up a two-way channel of communication with employees.
4. Support employee-owned devices with best practices that address a user-centered strategy and the inherent security issues around BYO.
5. Recognize that there is no one-size-fits-all solution for consumerization: The diverse roles and responsibilities in the enterprise come with a range of technology needs.
Step 1: Understand the Powerful Forces at Work

There are a number of driving forces continuing to shape consumerization, and leading the way is a changing workforce. Today’s employees are more technically savvy and sophisticated than ever before. If they feel that the technology options provided at work are not meeting their needs—or they perceive IT standards to be inflexible in any way—they have the technology know-how to find a workaround in an effort to be as productive as possible. This may be by using their own devices, downloading or using a personal cloud storage service, or engaging with social media so that they can work more efficiently. It’s convenient, certainly, but it can be in direct conflict with established IT security policies.

Cloud computing makes this even easier, with information and services accessible from anywhere, any time, using any device. For example, if an employee knows he may later need access to a file created on his work computer, he can easily store the document using his personal cloud service. Although he may be relying on that service primarily for personal use, he can upload his work documents and then access them from any device.

Younger Workers, Higher Expectations

Another important aspect of this changing workforce is age. Workers from Generation X, Generation Y, and beyond grew up using technology. In fact, college graduates of 2012 have never known a world without the Internet. This web-literate generation brings innovation and a fresh perspective to the workplace, yet they also want instant gratification—think instant messaging and immediate downloads. Fueling this tendency are the latest innovative devices, such as smart phones and tablets.

These employees are less willing to wait a few quarters, let alone years, for IT to equip them with the latest technology. They communicate using Twitter®, Facebook®, LinkedIn®, and Skype®, and many view e-mail as an old-school communication method. It’s a trend of accelerated technology adoption: what may have taken older generations a year or more to adopt, Generation X and Generation Y workers can adopt in a matter of months.

These dynamics apply not only to your workforce, but your customer base as well. Think about these numbers: A 2011 IDC study revealed that IT underestimated the number of information workers using consumer devices for work by nearly 50 percent and the use of social networks for customer communication by nearly 46 percent.

The bottom line? It’s likely that this is happening within your own organization, with or without your knowledge. By taking a proactive approach to consumerization, you’ll gain the visibility you need to identify the issues caused by unsecured and unmanaged technologies.
Step 2: Rethink User Computing

When it comes to end-user computing, most enterprise operations have traditionally taken a device-centered approach. This worked well when employees were using only employer-provided desktop PCs. Traditional client management practices focused on maintaining and securing the image on the PC, which was sufficient because the PC was usually connected to the corporate network. The monolithic image provided the operating system, applications, data, and personal settings the end user needed.

Shifting Focus from Devices to Users

Clearly, this approach is no longer sufficient to address today’s complex computing landscape and the countless number of employees working on consumer-grade devices. These devices pose IT challenges because they run different operating systems that may occasionally connect to the corporate network, but are constantly connected to the Internet. The devices also typically have no management framework and are accessing applications and cloud services that may or may not be provided by or qualified for use by IT.

To effectively meet the challenges of this dynamic landscape and truly embrace consumerization, your organization must rethink how it manages user computing. At the core of this new approach is the need to develop a user-centered strategy—one designed to optimize the computing experience and keep the user productive on any device, whether connected to the corporate network or not.

Simplifying with Centralized Management

One way to simplify and support a user-centered strategy is through centralized management. With centralized management, you can gain the flexibility and visibility you need to securely deliver the right computing resources to each user. You’ll have the ability to improve manageability and security by controlling operating system and application updates, as well as optimize data center resource usage.

You can do this by implementing a model in which you centrally manage the different layers of the Windows* operating system image and deliver those components to the end user based on context—device, location, role, time, and so on. To ensure a responsive, reliable experience with minimal latency, the majority of processing can be done locally on the end user’s device.

Moreover, many devices based on Intel technologies offer built-in management and security capabilities that help IT troubleshoot and remediate devices remotely, even if the operating system is not functioning. With hardware-assisted security features, you can gain added protection for users and corporate data that goes beyond what software-only solutions can provide. These added security capabilities deliver intrinsic support and peace of mind to organizations that are managing consumerization.

There are many technologies that can help with layering or compartmentalizing. For example:

- Applications can be decoupled from the underlying operating system and device using application virtualization and streaming technologies.
- Personalized settings can be persisted across devices and desktops with user virtualization solutions.
- Data can be made available from multiple devices using “follow-me data” or corporate file sharing solutions.
- Corporate e-mail can be accessed from multiple devices using Microsoft Exchange ActiveSync* technology.
- The operating system can be decoupled from the underlying hardware with client-side hypervisors for centralized management with local execution.
Step 3: Create an Inclusive Approach

In a business environment, there is no single solution for consumerization. What works well for one organization may not be enough for another. In fact, multiple approaches may coexist in a single environment, provided they are well designed and complementary. Intel believes that by starting with a user-centered strategy and then addressing both employee-owned and employer-provided devices, you can shape an inclusive approach to consumerization that is right for your organization.

It’s Less About Technology, More About People

Adopting a user-centered strategy starts with the people involved, rather than focusing only on the devices. And it means that IT must engage in a deeper level of communication with end users than ever before. For consumerization to work, you must move beyond the traditional, one-way communication model of IT-to-user to a more bidirectional process of communication.

For example, by engaging end users and key stakeholders in technology discussions early on, you will be able to gain a better understanding of the desired computing experience. What experience is the employee after, exactly? What are they using the technology for? For example, if you can move beyond the initial request for a “stylish new laptop” and ask some pertinent questions, you may find that the employee is simply seeking a portable model for business travel.

Whether your organization is exploring employee-owned devices, issuing employer-provided devices, or using multiple solutions, this inclusive communication approach is at the core of a user-centered strategy. When you embrace a two-way communication channel with employees, your organization will be in a stronger position to manage the challenges of consumerization while helping to improve morale and increase productivity across the business.
Step 4: Support Employee-Owned Devices

It’s no surprise that there are widespread security concerns about employee-owned devices. Allowing this technology into the enterprise poses obvious challenges to security and privacy, especially since IT can’t possibly protect what it doesn’t know about. There are universal concerns about device management and data protection, especially for lost or stolen devices. There are also concerns pertaining to budget, IT support parameters, legal implications, and the realities of managing multiple disparate devices.

However, if managed well, BYO programs do have the potential to offer significant benefits to employees and the business. For example, Intel implemented a personal device program in 2010 after several months of careful, comprehensive planning. Today, nearly 25,000 employee-owned smart phones are successfully supported—boosting employee job satisfaction and improving productivity. Equally important is the fact that Intel was able to strengthen security by eliminating the use of unsecured, unmanaged devices, with little to no increase in IT Service Desk calls. Furthermore, because of this experience with employee-owned smart phones and similar support models, Intel is now adding tablets to the program.

Ensure Success with Five Best Practices

Based on its successes, as well as lessons shared by customers and partners, Intel identified a set of best practices for supporting employee-owned devices in the enterprise. As you rethink your approach to consumerization, these best practices may help you develop a stronger user-centered strategy and address some of the inherent security issues around BYO.

1. Engage stakeholders
2. Update your security model
3. Decide on OS and devices
4. Plan deployment
5. Stay current with technology
1. **Identify and engage stakeholders** – Consider creating a master vision for your program by engaging and collaborating with all key stakeholders early in the process— from human resources and legal to IT, corporate services, and most importantly, end users. This is an ideal opportunity to define all the components of your BYO program:

- Decide which new devices your organization will support as IT-issued tools.
- Understand what types of new applications are needed to improve productivity.
- Clarify key program components.
- Work with human resources and legal to define the parameters of device ownership, such as service and support agreements, approval processes, privacy regulations, employee policies, regulatory controls, and fair use policies.

This best practice lends itself naturally to a user-centered strategy. As you engage in a two-way dialogue, you’ll be able to gather the feedback you need to clearly define these policies. It’s perhaps the most efficient way to gather the technical requirements you need and gain a clear vision of how to achieve the right computing experience.

Collaboration among the key stakeholders is also important. For example, Intel formed working groups that included policy-level decision makers across a range of disciplines, from HR, Legal, and Privacy to Corporate Services, Line-of-Business Owners, IT Engineering, and IT Information Risk and Security teams. These representatives influenced and guided the implementation process on behalf of their respective groups. Although each had a different objective, the group was able to better identify risks by working together.

One best practice that Intel IT found helpful was the use of profiling to create data security strategies. This was done by predicting likely forms of attacks using attacker profiling that looks at backgrounds, levels of determination, knowledge, and resources. Then, based on this information, Intel required that certain security controls be in place for personal devices to access corporate data, including:

- Two-factor authentication
- Secure storage using encryption
- Secure policy settings and restrictions
- Secure data transmission to and from the Intel network
- Remote wipe capabilities (where possible)
- Firewall and intrusion detection system (IDS) capabilities, and the ability to check for viruses (server side)
- Mobile device management (MDM) software to secure, monitor, manage, and support mobile devices over the network.

2. **Update your security model** – When you develop a security model for employee-owned devices, it’s smart to shift your focus into a broader vision: Instead of focusing solely on securing hardware devices, concentrate on protecting the corporate data that will be accessed by a range of devices. This includes determining the level of access to grant and implementing security controls such as authentication, data protection, antivirus, and governance.

It’s also crucial to train employees at the beginning of the program, as well as on an ongoing basis, on how to prevent issues and protect information on their devices. For example, it’s a good idea for employees to refrain from loaning out their devices or disclosing their user names and passwords, even to family members. By educating all employees on the risks of exposing corporate data, you can further enhance information security through behavior modification.
3. Decide which operating systems and devices to support – After you achieve buy-in from key stakeholders and create a security model, you can determine which devices to include. Before beginning this step, however, it is important to consider which operating systems your organization will support. Intel IT did just this; by focusing on the operating system first, the device decision-making process was made that much more efficient. To ensure that the technology choices wouldn’t overwhelm the IT staff, this process included a holistic assessment of the following components:

- Device evaluation and certification process
- Associated costs of supporting the new devices
- Available services, such as e-mail and calendar
- Support model

To minimize potential problems, Intel rigorously tested and automated the instructions that employees receive when their devices are activated. Intel also created an online forum and community that provides support to employees participating in the personal device program, which continues to be one of Intel’s most active forums.

When you’re determining which devices you’ll support, it’s important to remember that it’s not about granting users their every wish; it’s about your organization making an investment in a manageable set of options that can satisfy employees and work for IT.

4. Enable the technology and plan deployment – This step is about building the infrastructure that will work best for your organization to support devices. This includes considerations around software requirements, bandwidth options, management needs, and investment parameters.

Consider this fact: The recent influx of devices based on non-traditional operating systems is bringing a host of new security challenges to IT. End users are able to bypass native security mechanisms on these devices insecure, or the devices can encounter an attack and become infected, impacting the network. You can mitigate these risks using mobile device management (MDM) solutions or mobile application management (MAM) tools, which help ensure that these devices remain secure. The foundation for these technologies, Microsoft Exchange ActiveSync technology, delivers corporate e-mail to these devices without requiring them to join the domain. It also allows IT to set device security policies, such as password complexity and length, and settings for lockout, time-out, and remote-wipe capabilities that wipe either the entire device or just the corporate components if the device is lost or stolen.

In Intel’s case, the technology deployment process involved creating an easy-to-use Web portal for service requests, and then educating and training all parties about the new program—including managers, employees, and IT support staff. By carefully planning technology deployment and training within your own organization, you can help ensure that demand for the new program doesn’t outpace the ability to support program participants.
5. **Stay up-to-date with changing technology** – By staying on top of technology trends, you can better forecast what’s coming next and think about how it might fit within your infrastructure. One way to do this is by creating a turnkey evaluation process to assess new technologies and devices so that you can efficiently identify those you want to add to your program.

For this step, Intel found success by using an assessment process that focused on the following five key components:

- **Security** – Establishing security criteria can help you ensure that information is safe in transit and in use, and also that the device is protected from malware and in alignment with handheld policies. This includes features such as power-on password protection to prevent unauthorized access; content encryption capabilities for data the enterprise wants to protect; and device intrusion protection that uses the native device capabilities to prevent malware at the platform level.

- **Manageability** – Identifying manageability criteria will help you evaluate the device for both the enterprise and the consumer. This includes features such as enterprise management and MDM solutions; over-the-air (OTA) provisioning for applications; proactive monitoring support for health and status with autoconfiguration options and profiles; and backup and restore capabilities in the event of loss or transfer to a new device.

- **Productivity** – Productivity criteria pertains to features that affect the end user’s ability to complete tasks efficiently. This includes support contextual data; a blended social interface for accessing multiple accounts; and support for offline consumption for data and services.

- **Performance** – Establishing performance criteria, such as battery life, processor speed, and screen size, can contribute to the speed and functionality of the device. Features include support for a minimum of one full day of battery life; responsiveness for always-on or instant-on capabilities; and support for multiple radio frequencies or bands, such as four-band Global System for Mobile Communications (GSM). Another important factor is sufficient on-device storage and RAM.

- **Ease of use** – Although ease-of-use features can be subjective, you may want to consider a range of usability functions. This includes but is not limited to an intuitive user interface; easy updates to the operating system, firmware, and applications; fluidity of use when switching between tasks; and multiple input options.
Step 5: Find the Right Tool for the Job

In today’s business environment, there are diverse roles and responsibilities with a range of technology needs. Although a BYO model clearly has its strengths, it typically won’t meet the computing and productivity needs of all employees. In fact, most employees don’t want to bring their personal computing devices into the workplace. They expect their employers to provide them with the tools they need to do their jobs.

Part of rethinking your approach to end-user computing is recognizing that there is no longer a one-size-fits-all solution. Mobile employees may need a full-featured laptop with a companion device such as a smartphone or tablet, while other employees who do specialized business tasks require tools that are optimized for portability and long-term use. And professional office workers may need a full-powered desktop system that can handle any task. Companies must continue to provide business-class technology to equip their employees with the right tool for the job.

Fortunately, there is now a range of technology options for employees, compared to the limited options offered just a year or two ago. The difference is that today’s criteria for these devices are about more than function. To fully support a user-centered strategy, it is important to offer employees tools that meet the minimum requirements for responsiveness, security, and manageability and can be optimized for different roles, such as:

- Task workers, who require the on-the-go flexibility of business-class tablets
- Mobile workers, who need full-featured systems that are portable, with a strong battery life
- Office workers, who want powerful all-in-one devices, but may have space constraints

Greater Productivity through Fair Use Policies

With employer-provided devices come a responsibility to embrace and support fair use policies for all employees. Although fair use guidelines require some degree of management—such as regular updates and refinements—they will invariably help improve employee morale. In addition, by allowing reasonable personal use time and applications on employer-provided devices, employees are more likely to work at different times and from home, helping to drive productivity.

On-the-Go Convenience for Task Workers

For task workers, less is usually more. Whether it’s a nurse charting a patient’s condition or a shipping manager updating the status of an order from the warehouse floor, these workers often prefer the mobility of a portable device such as a tablet.

With the introduction of the Windows 8 operating system, new innovative tablets are coming into the market, giving you more options to support your task workers while lowering your total cost of deployment. For example, a wide range of Intel® processor-based tablets are now available with touch screens and peripheral support.

The Windows 8 Pro operating system is compatible with most enterprise environments, which further simplifies integration. Touch-enabled devices based on this new operating system can also be managed simultaneously with devices based on the Windows 7 operating system. Most important, these Intel-based devices all offer a variety of built-in security, manageability, and performance capabilities, as well as extended battery life and energy efficiency. Finally, these tablets deliver an array of Windows 8 experiences with a wide range of processor options, including Intel® Core™ vPro™, Intel Core, and Intel Atom™.
Sleek Meets Rugged: Full-Featured Systems for Mobile Workers

Unlike task workers, most mobile workers require a full-featured laptop and often rely on additional computing devices to provide convenient data access on any given day. Whether in an airport, at a hotel, or at a client’s location, these workers need flexibility and power. And while traditional business-class laptops offer all the necessary features, they are often bulky and cumbersome—less than ideal for workers on the go.

Today’s groundbreaking systems strike the ideal balance between performance, power, and mobility: They are rugged enough to withstand the rigors of business travel, while still appealing to mobile workers’ desire for a convenient, portable style. These innovative models include a range of choices based on Intel Core vPro processors that deliver the built-in security and manageability that IT requires, combined with the speed and stunning visuals that employees need to gain and share business insights at any time, from any location.

Ultrabook™ is Built for Business, Engineered for Security

One powerful example of a full-featured system is the Ultrabook™ device, inspired by Intel. Available in a growing portfolio of choices, this sleek, powerful device bridges the gap between form and function—with many models that are designed for business. A range of new models based on Intel vPro™ technology offer greater choice for business workers, with features such as the ability to wake instantly and a design that measures less than 1 inch thick. These business-class models are designed for workplace use and travel with stronger hinges, a hardened chassis, and extended battery life.

New Ultrabook convertible models offer even more as a two-in-one device, including a form factor with a detachable touch screen that easily converts into a tablet. Ideal for sales managers and C-level executives who may be currently using both a laptop and a tablet, this design gives mobile workers everything they want—and without having to carry two devices.

This innovative form factor delivers the best of both worlds: Employees get the sleek, thin device they want, while IT gets the convenient, budget-friendly option of equipping workers with and supporting a single device. And because the Ultrabook is based on the 3rd generation Intel Core vPro processor with embedded security, it is designed to better protect data and user identities while helping to keep threats out.
Compact Power for Today’s Office Workers

The impact of consumerization isn’t limited to mobile employees. Office workers are still going strong in today’s business world—whether they are sitting in a cubicle or in a home office—and they rely on desktop PCs to get their jobs done.

Innovation on desktop PCs is also moving at a rapid pace. Designed to enhance employee workspaces, these models are growing in popularity in large part due to their simplicity and clutter-free designs, but also because they’re based on Intel processors that provide the performance, security, and manageability needed in an enterprise environment. With the introduction of the Windows 8 operating system and its touch-enabled features, all-in-one devices powered by Intel Core vPro processors provide an even more responsive dynamic desktop for your office workers with compelling large-screen experiences needed to accommodate certain users and applications.

A Lack of Technology Choices Brings Risk

When given no compelling choices from their IT department, some employees may forgo employer-provided computers in favor of their own devices that they’ve purchased through traditional consumer channels. Unfortunately, many employees make these decisions without insight into their employer’s security and manageability policies. They also may not realize that some devices are inherently more ready to meet these requirements than others.
Embracing the Inevitable—Without Abandoning the Past

As the powerful force of consumerization continues to evolve, it's important to act now so that you can minimize risk. By rethinking your approach to user computing and shifting to a user-centered strategy, you can begin to align your employees’ at-home computing experience with the one they have at work. In turn, you can help improve employee job satisfaction and increase productivity—all while gaining greater security and control for IT. And you can do all of this by leveraging your existing investments in technology, applications, and training.

Gaining Compatibility and Flexibility

Intel architecture delivers the performance, security, and manageability you’ve come to rely on, and it’s prevalent across a range of computing environments. When you use Intel processor-based platforms running the Windows 8 operating system, you can trust that the solution will be compatible with traditional applications, peripherals, and drivers that span most enterprise environments today.

With the ability to leverage your past IT investments and take advantage of a trusted and familiar technology platform, you can design your approach to consumerization on a solid foundation that includes:

- Devices business users will enjoy
- Security and manageability IT requires
- Productivity that businesses value
- The broadest range of choices

Whether you draw upon Intel IT’s experience and best practices or integrate a growing number of new Intel processor-based devices into your organization, you’ll be better prepared to move your organization forward—and embrace the inevitable.

Intel® Technology and Windows® 8—A Compatible Combination

Seamlessly integrate Intel® processor-based devices into your computing environment

<table>
<thead>
<tr>
<th>Ultrabook™</th>
<th>Tablet</th>
<th>All-In-One</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility and style</td>
<td>Touch-first experience where flexible and reliable mobile computing is required</td>
<td>Performance and style</td>
</tr>
<tr>
<td>Supports touch-first and traditional keyboard &amp; mouse interfaces</td>
<td>Delivers Windows® experience to Intel tablet users</td>
<td>Large screens demanded by some users</td>
</tr>
<tr>
<td>Optimal blend of responsiveness, performance, and longer battery life</td>
<td>Increased security with hardware-enabled security from Intel®</td>
<td>Integrated touch capabilities on some models</td>
</tr>
<tr>
<td>Increased security with hardware-enabled security from Intel®</td>
<td>Increased security with hardware-enabled security from Intel®</td>
<td>Increased security with hardware-enabled security from Intel®</td>
</tr>
</tbody>
</table>

Plus Compatibility with Millions of Existing Software Applications, Peripherals, and Drivers
Resources for Learning More

To learn more about how to manage consumerization in your organization, visit the following web sites:

- For more information about consumerization, visit intel.com/consumerization.
- For more information about client security, visit intel.com/pcsecurity.
- For more information about Ultrabook for Business, visit intel.com/ultrabookforbusiness.
- For more information about Intel® Core™ vPro™ processors, visit intel.com/vpro.

Additional Resources

**Peer Research: Insights on the Current State of BYOD in the Enterprise**
Find out how IT managers across four countries view Bring Your Own Device (BYOD) in the enterprise. The research included 3,000 IT decision makers and 1,300 end users from Australia, Germany, South Korea, and the United States in an effort to understand how IT managers define BYOD programs, as well as the anticipated benefits and requirements for success.

**Consumerization of IT and Intelligent Desktop Virtualization**
Consumerization is forcing IT to rethink how they manage end-user computing. Read this paper to find out how Intelligent Desktop Virtualization helps IT managers embrace consumerization and thrive.

**Evaluating Ultrabook™ Devices for the Enterprise**
Find out what Intel IT discovered in its Ultrabook device evaluations. While consumer models can pose risks in the business, upcoming enterprise Ultrabook devices will include features that strongly support business usage models, especially in situations where employees need to constantly carry their computing device with them.

**An Overview of Consumerization: Embracing the Inevitable**
Get quick insight into consumerization with this animation. With the changing IT landscape, one-device-fits-all no longer holds. See how you can prepare for change and equip your employees with the right devices.

**IT @ Intel: Best Practices for Enabling Employee-Owned Smart Phones in the Enterprise**
Find out how Intel took a proactive approach to enabling personal devices in the enterprise with these eight best practices for a successful personal device program.
More from the Intel® IT Center

The Five Steps to Consumerization planning guide is brought to you by the Intel® IT Center, Intel's program for IT professionals. The Intel IT Center is designed to provide straightforward, fluff-free information to help IT pros implement strategic projects on their agenda, including virtualization, data center design, intelligent clients, and cloud security. Visit the Intel IT Center for:

- Planning guides, peer research, and vendor round tables to help you implement key projects
- Real-world case studies that show how your peers have tackled the same challenges you face
- Information on how Intel's own IT organization is implementing cloud, virtualization, security, and other strategic initiatives
- Information on events where you can hear from Intel product experts as well as from Intel's own IT professionals

Learn more at intel.com/ITCenter.

Share with Colleagues

This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED AS IS WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION, OR SAMPLE. Intel disclaims all liability, including liability for infringement of any property rights, relating to use of this information. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Copyright © 2012 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel Atom, Intel Core, Intel Sponsors of Tomorrow, the Intel Sponsors of Tomorrow logo, Intel vPro, and Ultrabook are trademarks of Intel Corporation in the U.S. and/or other countries.

Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries.

*Other names and brands may be claimed as the property of others.

1012/BC/ME/PDF-USA 328014-001

1 Gens, Frank, Danielle Levitas, Rebecca Segal. 2011 Consumerization of IT Study: Closing the “Consumerization Gap.” Unisys (July 2011).
4 Intel vPro technology is sophisticated and requires setup and configuration. Availability of features and results will depend upon the setup and configuration of your hardware, software, and IT environment. To learn more about the breadth of security features, visit intel.com/technology/security
5 No computer system can provide absolute security under all conditions. Built-in security features available on select Intel Core processors may require additional software, hardware, services, and/or an internet connection. Results may vary depending upon configuration. Consult your PC manufacturer for more details. Additional software, hardware, services, and/or an internet connection may be limited. Consult your PC manufacturer for more details. For more information, visit intel.com/technology/security
6 Security features enabled by Intel Active Management Technology (Intel AMT) require an enabled chipset, network hardware and software, and a corporate network connection. Intel AMT may not be available or certain capabilities may be limited over a VPN based on a host OS or when connecting wirelessly, on battery power, or while sleeping, hibernating, or powered off. Setup requires configuration and may require scripting with the management console or further integration into existing security frameworks, and modifications or implementation of new business processes. For more information, see intel.com/technology/security
7 For more information, see intel.com/technology/security
8 Intel vPro technology is sophisticated and requires setup and configuration. Availability of features and results will depend upon the setup and configuration of your hardware, software, and IT environment. To learn more, visit intel.com/technology/security
9 Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests such as SYSmark and MobileMark are measured using specific computer systems, components, software, operations, and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more information go to intel.com/performance
10 Ultrabook products are offered in multiple models. Some models may not be available in your market. Consult your Ultrabook manufacturer. For more information and details, visit intel.com/ultrabookforbusiness
11 Intel vPro technology is sophisticated and requires setup for business activation. Availability of features and results will depend upon the setup and configuration of your hardware, software, and IT environment. To learn more, visit intel.com/technology/security
12 No computer system can provide absolute security under all conditions. Built-in security features available on select Intel Core processors may require additional software, hardware, services, and/or an internet connection. Results may vary depending upon configuration. Consult your PC manufacturer for more details. For more information, visit intel.com/technology/security
13 No computer system can provide absolute security under all conditions. Built-in security features available on select Intel Core processors may require additional software, hardware, services, and/or an internet connection. Results may vary depending upon configuration. Consult your PC manufacturer for more details. For more information, visit intel.com/technology/security