IT@Intel White Paper

Intel IT
IT Best Practices
IT Consumerization and Employee Productivity
December 2011

Best Practices for Enabling Employee-owned Smart Phones in the Enterprise

We have enabled almost 15,000 employee-owned smart phones over an 18-month period—providing increased access to information and IT services to improve flexibility and boost productivity.

David Byrne
Handheld Technology Specialist, Intel IT

Rob Evered
Information Security Specialist, Intel IT

Executive Overview

To support IT consumerization, Intel IT is focused on delivering services to a range of corporate- and employee-owned devices. By taking advantage of a combination of technologies and trends—such as ubiquitous Internet connectivity, virtualization, and cloud computing—we have an opportunity to redefine the way we provide services to meet changing user requirements.

In early 2010 Intel IT implemented a personal device program, which allows employees to use their own smart phones to access corporate data. We have enabled almost 15,000 employee-owned smart phones over an 18-month period—providing increased access to information and IT services to improve flexibility and boost productivity.

Enabling employee-owned devices in our environment presented significant security and privacy challenges. Working closely with Intel Legal and Human Resources (HR) groups, we developed an implementation plan, created the necessary policy and technical infrastructure, and rolled out the program. Although it took many months to get to roll-out, the program itself is quite simple: Employees request service online, agree to the terms of the service, obtain manager approval, and receive configuration instructions automatically.

Based on our experiences, we have identified eight best practices for creating a personal device program that meets our information security standards:

- Identify and engage stakeholders early in the planning process to address their concerns and get input to create a master vision for the program.
- Engage end users to determine how they want to use personal devices and what they expect from IT with regard to these devices.
- Develop a security model that adequately protects corporate data at reasonable effort and cost.
- Decide which devices to implement; for example, we decided to support specific OSs rather than specific hardware models.
- Address legal and HR concerns by creating a comprehensive but flexible service agreement that is legally viable in the countries where it will be implemented.

Contents

IT@INTEL

The IT@Intel program connects IT professionals around the world with their peers inside our organization – sharing lessons learned, methods and strategies. Our goal is simple: Share Intel IT best practices that create business value and make IT a competitive advantage. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

- Enable the technology by building out infrastructure, creating an easy-to-use Web portal for service requests, and educating managers, employees, and IT support staff about the new program.
- Plan the deployment so that demand for the new program does not outpace the ability to support program participants.
- Stay up to date with changing technology by monitoring developments in the mobile OS marketplace, reviewing consequent impacts on the program, and updating the service agreement as necessary to cover new device types, capabilities, and features.

Internal data indicates that employee productivity and job satisfaction have increased as a direct result of implementing personal devices in the enterprise. Employees send approximately 2.27 million business-related e-mail messages each quarter from corporate and personal devices. More importantly, employees report time savings of about an hour per day by using personal devices.

Additionally, formalizing implementation of employee-owned smart phones has improved enterprise security by eliminating unsecured, unmanaged personal devices from our environment. In the future, as device security matures, we anticipate supporting an increasing variety of personal devices and the services available to them using our best practices and policies already in place.

BACKGROUND

Intel IT determined that formalizing the implementation of employee-owned devices in our computing environment could actually improve enterprise security by eliminating use of unsecured, unmanaged devices. We are therefore actively integrating personal devices, including smart phones and tablets, into our environment. In so doing, we are transitioning away from a traditional client computing model that supports a limited number of device types—mostly desktop and laptop PCs—toward a new model. Intel envisions a seamless, consistent experience across devices in what we call the "Compute Continuum."

We have supported handheld devices in the enterprise for several years, but only in the context of a corporate model whereby Intel purchases devices for employees and pays for the service plan, and only when there is a strong business need for the devices to facilitate job functions.

The benefits associated with integrating personal devices into our enterprise environment include enhanced employee productivity and job satisfaction, and greater business agility provided by a wide array of usage models, without significantly increasing IT's total cost of ownership (TCO). For example, internal data shows that employees save almost one hour per day on average using handheld devices while the number of related Service Desk tickets per user has actually decreased.

Extending support to employee-owned devices presented significant security and privacy challenges. Stakeholders, including Intel Legal, Human Resources (HR), and Information Security groups, had legitimate concerns that needed to be addressed from the very beginning of the project.

We also needed to develop new support models that addressed the unique aspects of employee-owned devices compared to corporate-owned devices. These issues ranged from simple device ownership to lack of IT control over device refresh rate and patch management to maintaining both personal and corporate information security.

The foundation we have laid in implementing our personal device program will accelerate future deployment of new device types.

BEST PRACTICES FOR DEPLOYING A PERSONAL DEVICE PROGRAM

Intel deployed a personal device program in early 2010 that enables employee-owned devices to access enterprise data while maintaining compliance with corporate information security standards. Rather than securing hardware, our approach focuses on protecting the data that the hardware is accessing. We provide tiered services based on the security controls in place on each device.

Our personal device program is simple: When employees want to use their own devices to perform their jobs, they submit a request online, receive manager approval, and automatically receive instructions about how to configure their devices and start using the service. During the sign-up process, employees agree to the terms of the service that explains how employee conduct guidelines apply to personally owned devices and how the program balances employee privacy rights with corporate data security concerns.

Our experience allowed us to develop a set of best practices for implementing a personal device program, as outlined in Figure 1.

Best Practice #1: Identify and Engage Stakeholders Early in the Planning Process

Integrating employee-owned devices into our enterprise environment was more than a technology exercise. Because it affected many different groups across Intel, early in our planning process we identified an extensive team of stakeholders:

- Intel HR group
- Investigations team
- Intel Legal group
- IT Engineering team
- Privacy team
- Corporate Services group
- Line-of-business application owners and business groups who were looking at future capabilities
- IT Information Risk and Security team

The handheld product manager and the IT Information Risk and Security team led a newly formed working group that included policy-level decision makers and other representatives from each of these areas. The diverse members influenced and guided the implementation process according to their organizations' functions. Although each representative had different objectives, the working group was able to identify risks that only became apparent through collaborative effort.

Best Practice #2: Engage End Users

Because one of the goals of integrating employee-owned devices into the enterprise was to increase employee productivity and job satisfaction, we needed to find out exactly what employees wanted to accomplish with their devices. To investigate employee behaviors and preferences, we engaged with employees directly, using a blog to discuss the creation of a new IT consumerization policy.

As we set up the blog, we worked closely with Intel Legal and HR groups. We wanted to avoid giving employees the impression that discussing policy in an unconstrained environment meant that responses would be perceived as policy itself. We needed to set clear expectations in our communications that Intel IT was not making promises or firm statements about policy. We were careful to keep our tone conversational and honest, as illustrated by the following example:

> *"Over the next month we will be posting questions about how you believe Intel should handle the consumerization issue.*
>
> *Your feedback will be read by experts and decision-makers and may inform a future consumerization policy."*

We engaged a communications specialist to help write questions with employee behavior in mind. It was important to craft questions in

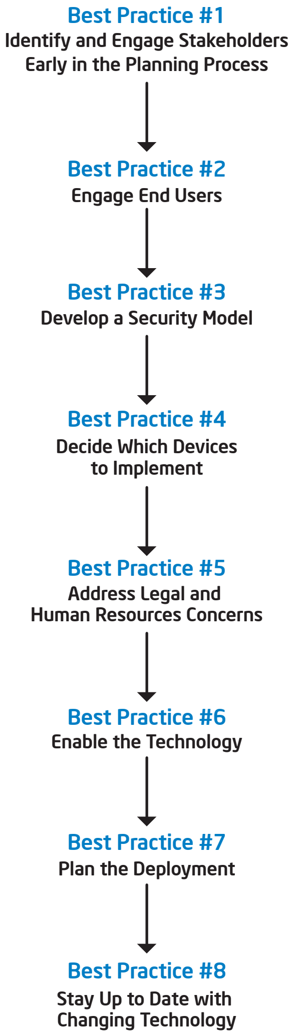

Figure 1. Intel IT formalized a set of best practices for implementing a personal device program based on a planning process that covered each of these areas comprehensively.

a way that would elicit meaningful responses. High-level questions we asked included:

- Why do you want to use your own device(s) for work?
- What would you give up to use your device for work?
- What does your personal device do that helps you work?

Many of our questions probed subtle distinctions: Asking about the applications required for work and about functionality might have seemed redundant, but people interpreted these two questions differently and provided different responses—which helped create a broad picture of usage patterns and preferences. In this particular example, applications allude to functionality but also reveal very specific solutions, while functionality confirms the overall preference or perceived need for a general task such as calendaring or e-mail.

Participation in this dialogue underscored employees' desire to use personal devices to perform their jobs—more than 8,000 employees responded. In fact, employee response was so enthusiastic and informative that we extended the life span of the blog from one month to six months.

Sometimes responses to our questions shed new light on assumptions we had made about how people worked. For example, two sales representatives with essentially the same job responsibilities had very different device preferences. One was adamant that he needed a device that could download applications, get e-mail, and show locations of airport lounges and wireless hotspots. His counterpart complained about having to use a device with extraneous features—he simply wanted a mobile phone that could make calls and had long battery life.

Overall, we gleaned important information that guided policy definition and technical implementation:

- **How** employees were already using personal devices
- **Why** they were using them
- **What** they expected from IT in regard to these devices

Best Practice #3: Develop a Security Model

Information security is critical, and it can be expensive. We developed a security model for employee-owned devices that enables us to maximize return on investment (ROI) by providing appropriate levels of protection for different types of Intel data. Our security model has three key elements:

- **Levels of access.** Because certain types of data are more sensitive and valuable, not all employees—or devices—have access to all data.
- **Security controls.** Each level of access requires a different set of security controls. The more security controls a device has, the greater number of corporate services it can access.
- **Attacker profiling.** Attackers have different backgrounds, levels of determination, knowledge, and resources—all of which affect the threat they pose to data. Predicting likely forms of attack helps us assess strategies for improving data security.

We created an algorithm that mathematically correlates these three components to help us determine which corporate data can be securely accessed by employee-owned devices.

LEVELS OF ACCESS

We defined five levels of access to data and services, as shown in Figure 2. Access to public data, such as that available on the Internet, requires the least amount of security. It would not be cost effective to encrypt this type of information. At the other end of the spectrum is access to the complete range of IT services. This requires the highest number of security controls because it is equivalent to the level of access we grant to a mobile business PC that we manage inside the corporate environment. The "managed equivalent" level of access is more expensive to deploy and manage.

Levels of access are cumulative. For example, devices granted intermediate access also receive basic, slightly confidential, and public access permissions.

SECURITY CONTROLS

Security controls are features of a device—either native in the OS, added with software solutions, or provided by IT infrastructure or device management—that result in appropriate data security. Each increasingly protected level of access, from public to managed equivalent, requires a greater number of controls to enhance overall security. Our goal is to balance the cost of security controls with levels of access to achieve maximum ROI.

Security Control Categories

We have defined four categories of security controls for devices:

- **Authentication.** These controls are associated with how users authenticate to devices and how devices and the user are authorized to access back-end resources. Examples include the ability to hold and protect certificates, enforce passwords, and support single sign-on.
- **Data protection.** These controls protect data both in transit and when stored on the device. Examples include encryption, preventing non-authorized applications from accessing data, and the key ability to remotely wipe the device if the device is lost.
- **Malware.** These controls address malware used by attackers to steal data. In our experience, most malware attacks on smart phones target its ability to send text messages and make high-cost calls, not the data stored on or accessed by the device. In light of cost justification, we rely primarily on the built-in malware controls of each mobile OS and the ability to inspect data sent back to the enterprise on the infrastructure side.
- **Governance.** These controls address legal and HR issues such as device mobile management, configuration compliance, monitoring, and eDiscovery. We apply governance controls as a single baseline after considering requirements for all countries. We are trying to minimize local and regional differences in order to streamline our support structure and cost.

We first determine how many security controls are necessary for a particular access level, and then we use that information to evaluate a mobile OS. For example, if the OS meets the required number of security controls for intermediate access, we can safely grant that access level to the device. If the number of security controls is lower than the required number of security controls, we reject the OS or add software that addresses security control gaps.

ATTACKER PROFILES

When data is threatened, it makes a difference *who* is threatening it. We have defined four attributes to help us profile attackers and determine the level of threat they pose.

- **Type.** Ranges from people who are not computer savvy and cause unintentional mischief to disgruntled individuals or organizations with intent to cause harm.
- **Determination.** Ranges from individuals with no determination—such as simple curiosity or accidents—to individuals who are so determined they don't care if they get caught.
- **Resources.** Ranges from no resources—such as money, hacker club memberships, underworld contacts, and computing resources—to unlimited resources.
- **Available tools.** Ranges from attacks that have never been attempted and for which no tools exist—posing less risk—to attacks that have already been successfully implemented and for which easy-to-use point-and-click tools exist—posing higher risk.

In profiling attackers, the more precise our definitions, the greater our ability to enhance our security position and verify that a device has sufficient security controls to protect against the most likely types of attacks.

- If a child found a smart phone left in a taxi, it is highly unlikely that this would pose a threat to Intel data because the child has no motivation, determination, or resources. Virtually any device, even those with only a few security controls, would be protected in this scenario.
- If a thief intent on harming our company stole a smart phone, a data breach would be much more likely unless the device had a large number of security controls.

Attacker profiles simply provide information about who the attacker could be. Attacker profiles do not vary based on the data, the device, or the location of an attack.

Ranking Attacker Attributes

To create attacker profiles, we assign a rank to each of the four attributes—type, determination, resources, and available tools. We then apply a mathematical algorithm—not a direct summing or averaging procedure—to these four attribute rankings to derive an "attacker profile total." Figure 3 compares two sample attacker profiles based on the rankings of the four attributes.

In the figure, Attacker A has a low attacker profile total because the attribute rankings are all quite low. This profile represents an attacker who is experimenting, has no determination, and has very few resources or tools with which to accomplish an attack. Attacker B poses a higher level of threat. This attacker might be a disgruntled individual with determination as well as resources and access to tools.

DETERMINING SECURITY RISK

We use the number of security controls on a device and attacker profile totals to determine the appropriate level of access for a particular device.

- **Step 1.** We determine the types of attackers likely to target a particular device and derive attacker profile totals using our algorithm.
- **Step 2.** We compare attacker profile totals to the number of security controls on a device.

If the controls on the device are greater than the attacker profile total, we consider the data that the device is accessing to have an appropriate level of protection in place. If the attacker profile total is greater than the security controls, the data that the device is accessing is at risk.

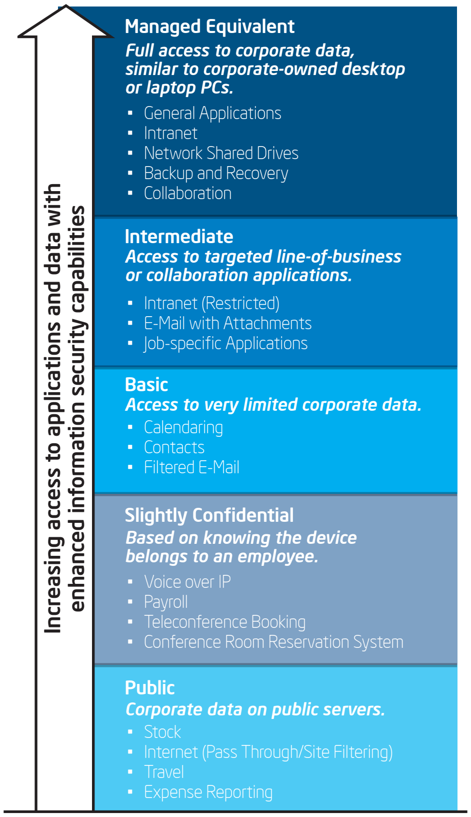
Increasing access to applications and data with enhanced information security capabilities
Managed Equivalent
Full access to corporate data, similar to corporate-owned desktop or laptop PCs.
▪ General Applications
▪ Intranet
▪ Network Shared Drives
▪ Backup and Recovery
▪ Collaboration
Intermediate
Access to targeted line-of-business or collaboration applications.
▪ Intranet (Restricted)
▪ E-Mail with Attachments
▪ Job-specific Applications
Basic
Access to very limited corporate data.
▪ Calendaring
▪ Contacts
▪ Filtered E-Mail
Slightly Confidential
Based on knowing the device belongs to an employee.
▪ Voice over IP
▪ Payroll
▪ Teleconference Booking
▪ Conference Room Reservation System
Public
Corporate data on public servers.
▪ Stock
▪ Internet (Pass Through/Site Filtering)
▪ Travel
▪ Expense Reporting

Figure 2. We control security costs by defining levels of access to data; each level provides appropriate protection, but no more. Our goal is to avoid paying for security we don't need.

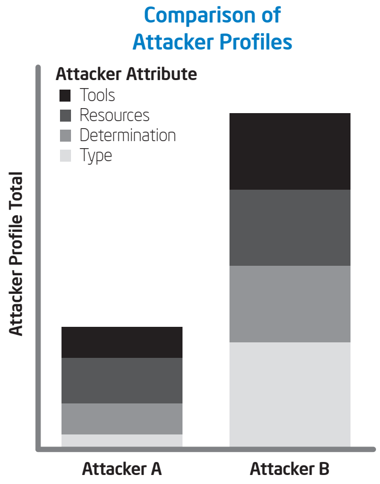

Figure 3. We derive an attacker's profile total using a mathematical algorithm to correlate the four attribute rankings.

Figure 4 illustrates this comparison. "Attacker Profile A" represents an attacker with a low profile total. Comparing it to the security controls available on device #1, which has public access, and device #2, which has intermediate access, reveals that both devices have more security controls in place than the attacker profile total. Therefore, this type of attacker poses a very low security risk to Intel data.

In contrast, "Attacker Profile B" represents an attacker with a much higher attacker profile total. Security controls for device #1 fall well below the attacker profile line—indicating that an attack would more than likely be successful. However, device #2 is protected because its security controls are still greater than Attacker Profile B's attacker profile total.

For data to be at minimal risk, a device's security controls must meet or exceed the threat level, as well as meet or exceed the access level requirements for the service or data being accessed.

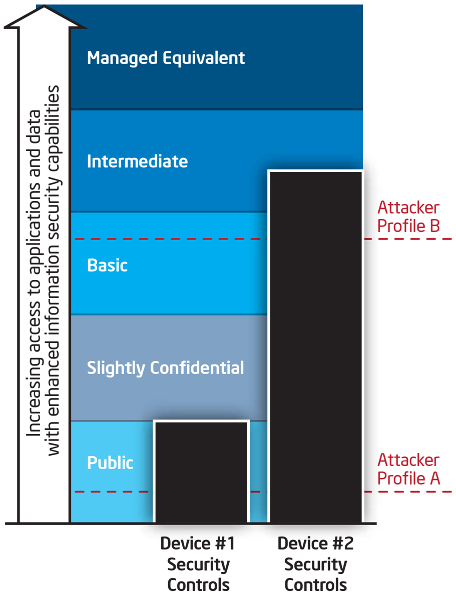

Figure 4. Comparing the security controls required for a level of access to the attacker profile total enables us to determine if we have an appropriate level of protection in place for a given device.

Using our security control and attacker profile matrices, we determined that we could securely grant access to the personal devices we currently support. We require certain security controls to be in place for personal devices to access Intel data:

- Two-factor authentication to access push e-mail
- Secure storage using encryption
- Security policy settings and restrictions
- Secure data transmission to and from the Intel network
- Remote wipe capability (where allowed)
- Firewall and Intrusion Detection System (IDS) capabilities on the server side of the connection
- Mobile device management (MDM) software that can secure, monitor, manage, and support mobile devices over the network
- The ability to check for viruses from the server side of the connection

Our security model, including attacker profiling, is also useful if a new type of threat emerges. Using our matrices, we can quickly create an attacker profile to determine if data remains adequately protected or if we need to implement further security controls.

Best Practice #4: Decide Which Devices to Implement

Once we achieved initial buy-in from all stakeholders, gathered information from employees, and developed a security model, we needed to decide exactly which devices to support and how to enable enterprise services effectively. We considered an array of factors that clarified our goals and how we would achieve them:

- Device evaluation and certification process
- Associated costs with supporting new devices
- Available service plans
- Support model

EVALUATION AND CERTIFICATION

Intel's original program for corporate devices supported three mobile OSs and used 70 service providers worldwide. As we considered enabling personal devices in the enterprise, we had to address the significant potential for overwhelming the IT Service Desk with requests for device support. For example, about 250 different smart phone models will be released in 2011, on seven or eight of the most popular mobile OSs. On average, each OS has three active versions in use at any given time.

When a new device is released in the marketplace, employees naturally want to buy it and would expect the personal device program to support it. However, given the high number of models and OSs, the traditional IT approach of certifying each device and OS version would result in about 500 certifications per year. Traditional IT methodologies cannot possibly support this aspect of consumerization without a more efficient process.

We developed a certification process focused on each OS and how it interacts with the enterprise; we do not validate at the hardware or service provider level. When a new OS or a new OS version becomes available, we review all technical, stakeholder, and business criteria to decide if it can safely be enabled in our environment.

The certification process results in a position statement that indicates whether or not we will support the new OS or OS version. We make these position statements available to employees through our handheld Web portal, so that employees can anticipate which devices they can and cannot use with the personal device program.

Using this certification process, we decided to support five OSs for both personal and corporate devices. We selected these OSs because they either supported mature security features—including password, remote wipe, policy enforcement, and encryption—or they supported a software-based encryption container that enabled us to grant them access to enterprise e-mail, contact, and calendar services in a secure manner.

ASSOCIATED COSTS

We knew that integrating more devices, service plans, and employees into our environment would incur development and support costs. We needed to determine how much it would cost Intel to enable the personal device program and balance the cost with ROI, which included the value of increased business agility, employee productivity, and employee satisfaction as well as enhanced security.

To estimate costs for the personal device program, we looked at the costs associated with our corporate device program. As shown in Figure 5, the service plan accounts for about 80 percent of TCO, while IT support and device acquisition are minor factors.

Because we would reap the business benefits of enabling personal devices for about 8 percent of the total cost, we decided to implement the personal device program. Employees would carry the majority of the costs, paying for both the device and the service plan.

Our current approach—supporting five handheld device OSs in the marketplace for both corporate- and employee-owned devices—has further minimized the cost of IT support. However, for our corporate devices, even when we supported only a single major mobile OS, we had to create three different engineering designs to accommodate different OS versions. Now that we support five OSs, all of which have differing security capabilities, we will continue to streamline development of services.

Adding a Hybrid Funding Model

About three months after we launched the personal device program, we were contacted by employees who were already using corporate devices but wanted to choose phones with more features and were prepared to pay for them. We created a hybrid funding model: Because the device was integral to their job functions, Intel would continue to pay for the service plans. The three funding models are compared in Table 1.

The hybrid option is not available in all geographic regions because of differences in law. Additionally, some suppliers are not allowed to split the device from the service plan.

AVAILABLE SERVICES

We provide push e-mail, calendar, and contact services—plus other collaboration tools such as instant messaging—to all supported OSs on both corporate and personal smart phones. Providing the same set of services simplifies both IT support efforts and program usability. Some smart phones have only a basic level of access to these services (see Figure 2), as natively they are less secure. For example, although devices with basic access can receive and send e-mail messages, they were not allowed to receive e-mail attachments when we launched the personal device program in 2010. These devices have matured to integrate more enterprise controls and therefore now receive e-mail attachments.

As more powerful, secure devices become available, we intend to expand the services available to personal devices, such as line-of-business applications. We are currently exploring providing Voice over IP (VoIP) and Wi-Fi* access to the Intel network to personal devices.

SUPPORT MODEL

Although we were adding a large number of devices to the enterprise, we did not want to significantly add to our IT support load. We took advantage of the "socialized self-support" model: Employees who bring in their own devices to the office are savvy about how their devices work and have more psychosocial ownership of these devices. As a result, they are much more likely to try—and succeed—at solving technical problems on their own instead of calling the Service Desk. In fact, we have discovered that because employees own the device, they are actually helping IT by identifying possible security threats and letting us know about them.

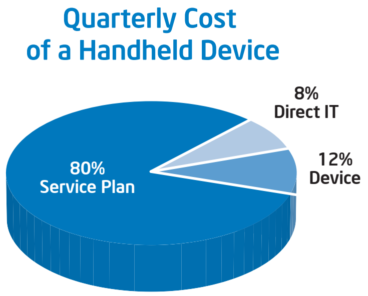

Figure 5. Direct IT costs account for only 8 percent of the total cost of a corporate device; the majority of the cost is the service plan. With personal devices, employees would carry the majority of the costs, paying for both the device and the service plan.

Table 1. Handheld Device Funding Models

	Device	Service	Participation Level
Corporate	Ⓒ	Ⓒ	35%
Hybrid	Ⓔ	Ⓒ	10%
Personal	Ⓔ	Ⓔ	55%

Ⓔ Employee-Funded Ⓒ Corporate-Funded

We created an online forum and community that provides support to employees participating in the personal device program. This online community is discussed in more depth in "Best Practice #6: Enable the Technology." This new social support forum is now the most actively used and technically savvy social forum at Intel.

To minimize potential problems, we also rigorously tested and automated the instruction set employees receive when their devices are activated.

Best Practice #5: Address Legal and Human Resources Concerns

Allowing employees to use personal devices to access corporate resources raises important legal, HR, and policy concerns. We needed to address these issues before we could launch the personal device program. We did this by writing a service agreement that employees must agree to before participating in the program and by incorporating manager approval into the sign-up process.

SERVICE AGREEMENT

All Intel employees who use handheld devices, both corporate and personal, are required to agree to the terms of the service agreement.[1] The agreement reminds employees of obligations in this new technical landscape.

In general, the service agreement addresses how employee conduct guidelines apply to personally owned devices and how the program balances employee privacy rights and corporate data security concerns. It also spells out how the use of personal devices impacts the way employees work and the implications that follow. We use the agreement to remind employees about security, specific to personal devices.

The agreement is written in plain language so that employees can easily understand it. The agreement does not discuss specific technologies or products, and the terminology is general enough to remain applicable as technologies change.

Service Agreement Topics

The agreement complements and links to Intel's terms and conditions of employment and other policies where appropriate. By telling employees what to expect, they can make informed choices about whether to participate in the personal device program. Some of the specific topics covered in the agreement include the following:

- Sign-up and registration. A requirement to register all devices accessing Intel enterprise services (e-mail, calendar, contacts, and other enterprise services)
- Data protection.
  - A requirement to protect Intel's intellectual property and information assets according to Intel's standard company policies regarding data storage, retention and backup, encryption, and disposal of the device.
  - A requirement to protect the Intel network from malware and other threats.
- Security enforcement. Guidance and notice about the methods Intel may use to help protect company data and confidential information on the device—including certain types of monitoring, inspection, mandatory remote wipes, disconnection, and so on.
- Policy compliance.
  - A requirement of compliance with Intel's standard policies while using devices, including its HR guidelines, wage and hour requirements, code of conduct, and software use and licensing policies.
  - A statement of the consequence for violation of these policies.
- Resources and support. Information about where to get support, who is responsible for hardware and software support, what to do if the device is lost or stolen, and how users can find additional information.

We carefully considered the tone of the service agreement as we wrote it. There are actions we have the right to perform—such as remote wipe of a device under certain conditions—and actions we want employees to perform—such as returning an old corporate-owned phone to Client Services when a new phone is purchased. However, taking a dictatorial tone in the service agreement would be counter-productive because we want to create a sense of collaboration between employees and IT. We tried, therefore, to make the controls practical, achievable, and enforceable.

Service Agreement Effect on Security

One encouraging sign that we have taken the right approach to the service agreement is that it has generated a dialogue between employees and IT. Employees proactively contact us about vulnerabilities, asking if a particular threat affects them.

Because employees own the devices, they have a genuine interest in security. We believe this is a new development in behavior and underscores how personal devices can actually increase information security in the enterprise.

MANAGER APPROVAL PROCESS

Managers are required to approve pushing Intel data to both corporate and personal devices. Corporate devices are issued when a manager indicates that the employee has a business need for the device. For personal devices, manager approval indicates that the employee does not require a personal device to perform job duties, but that such a device may increase the employee's productivity and flexibility during work hours and can assist in achieving work-life balance. We provide a list of frequently asked questions (FAQs) for all funding models so that managers fully understand the implications of approving the device.

We must consider the impact of granting use of personal devices on different types of workers, such as exempt, non-exempt, and contingent workers. Issuing personal devices to non-exempt employees requires special manager consideration. Because handheld devices are more convenient to access than mobile business PCs, it may be more likely that employees will use a personal device during off hours. Our service agreement reminds

[1] Referred to in some previous IT@Intel white papers as the "end-user license agreement" (EULA).

non-exempt employees that time worked, regardless of location, is compensable and that they are obligated to record time accurately. Managers must consider and accept their responsibility for making sure employees are correctly recording their work time.

We do not currently allow contingent workers (contractors) to participate in the personal device program. If they require handheld devices, the devices must be corporate-owned. We enacted this restriction because if we allowed contingent workers to use personal devices, the devices could be owned by them or by the staffing agency. Asking contingent workers to sign an agreement for a device owned by another company can make policy enforcement complex.

Best Practice #6: Enable the Technology

In addition to addressing the policy aspects of the personal device program, we also needed to address the technological aspects of implementing the program. These included the physical infrastructure that would support the program and the Web portal employees would use to order services. Once the pieces were in place, we ran a pilot project to test and tune the program, and provided training to employees, managers, and Service Desk personnel about the program.

INFRASTRUCTURE

Implementing support for five mobile OSs associated with personal devices required several modifications to our infrastructure, such as additional firewall controls. This was necessary because each of the mobile OSs had different security features, and some were more protected than others.

The methods we use allow as much data synchronization as possible without introducing unacceptable risk. The same approach can apply beyond synchronizing e-mail to other types of corporate data, such as application data.

Although currently both corporate and personal devices such as smart phones use the cellular network exclusively on Intel campuses, we are actively pursuing allowing such devices to use the Intel enterprise Wi-Fi network to further enable employees at work.

WEB PORTAL

We developed an intranet site to support the personal device program, with the goal of accelerating and streamlining adoption. Employees who are interested in participating in the program visit the Web site, which automates the sign-up process and provides other helpful information.

During sign-up, employees are presented with the service agreement; after they accept the terms, the system contacts their managers for approval. Employees also provide other necessary information such as device type and carrier service.

On the back-end, we built in automated accounting and developed an engine that sends instructions on how to configure devices. The engine delivers these instructions directly to employees and, whenever possible, we provide auto-configuration "over the air" to devices.

Some business units, such as manufacturing, restrict the use of personal devices due to more stringent security requirements. This additional control is possible by using the manager approval step in the ordering process.

Additionally, the Web site answers FAQs, provides instructions on what to do with old phones, and helps employees compare various device options, as shown in Table 2.

We publicize the program to employees through the internal Intel news service and other channels.

Table 2. Intel employees can use the information on our personal device program Web portal to compare smart phone features.

Feature	OS #1	OS #2	OS #3	OS #4	OS #5
E-mail	✓	✓	✓	Additional security software may be required, depending on the supported device	
Calendar	✓	✓	✓	✓	✓
Contacts	✓	✓	✓	✓	✓
Global Positioning System (GPS)	✓	✓	✓	✓	✓
Wi-Fi* Allows you to connect to your home network or public Wi-Fi in airport or coffeeshop, and other areas	Varies	Varies	Varies	✓	✓
Internet Usability	Good	Varies	Varies	Best	Best
Internet Applications Examples: mapping applications, currency converters, and so on	Good	Good	Good	Better	Best
Intel Intranet Availability	Some Available	✗	✗	✗	Some Available
Business Application Availability Examples: Instant messaging, bridge speed dialer, and so on	More Available	Some Available	Some Available	Less Available	Some Available
Battery Life Standby/talk	Best	Good	Good	Good	Good
Global Roaming Capability	Varies by Rate Plan				
Tethering Connect your phone to your laptop and use the phone as a modem to connect to the internet (like a wireless data card). Performance varies by phone model and service provider network speed.	✓	Varies by Country/Service Provider			

Table 3. Results of Personal Device Pilot Project

Metric	Goal	Actual Result
Estimate employee interest based on response rate	>50%	88% saturation (141 active out of 160 invitations)
User understanding of service agreement, according to survey results	80% positive response	100% understood
Ability to easily sign up using new tools	No showstoppers	100% agree
Effective manager/employee communications, according to survey results	90% positive response	92% positive interaction

Community Forum

Our Web portal features a community forum, which mirrors social support in the consumer market. We employed Intel's social media intranet site, Planet Blue, to accommodate this, enabling program participants to help each other instead of calling the Service Desk with questions.

This forum is the most popular discussion venue at Intel. Community members discuss popular personal device applications and share technical support to solve a range of issues. This is a significant departure from traditional support models in which IT educates users. Peer support is often more efficient because, in many cases, employees share new applications and solutions before IT is aware of them. The discussion forum is searchable, so that once a problem is resolved, future program participants can benefit. To date, more than 800 users have contributed about 3,000 posts.

PILOT PROJECT

We wanted service ordering and device configuration to be a seamless and easy process so that even non-technical employees could participate. We rigorously tested all aspects of the personal device program and subsequently launched a pilot project. We invited 160 employees to participate, with the following goals:

- Test the service agreement for acceptance and understanding, and request feedback.
- Validate the demand level and understand capacity needs.
- Verify that the process for requesting service is clear and easy to follow.
- Validate our expectation that employees are able to configure their own smart phones.
- Confirm that the automated communications work correctly for employees, managers, and business groups.

The results of the pilot project were very encouraging, as shown in Table 3. We had a high level of active participation, as well as a high level of satisfaction with the service agreement and the process as a whole.

Results for our personal device program continue to be positive; a recent user survey revealed that 94 percent of participants are satisfied with the program.

EMPLOYEE, SUPPORT STAFF, AND MANAGER TRAINING

We provided training to participants about the program, the service agreement, and how to protect Intel information on personal devices.

For example, we learned from the blog that about two-thirds of employees would loan their personal devices to family members—even if the devices stored Intel data. We used Planet Blue to convey awareness and education to employees about the risks that such behavior poses to Intel. By improving employees' understanding of risk, we enhanced information security through behavior modification.

We also discovered that Service Desk agents required training to answer program participants' questions about the service agreement. We developed specific FAQs to train our Service Desk agents and participants in the personal device program.

Finally, we provided managers with materials, such as FAQs, that helped them understand the new program, the costs that might be associated with it, and their roles and responsibilities.

Best Practice #7: Plan the Deployment

After we completed the pilot project and put the service agreement in place, we prepared for program deployment. We used a typical IT rollout process:

- We verified that capacity was sufficient to meet demand. Capacity included both infrastructure capacity and Service Desk capacity.
- We established critical success and operational indicators, and closely monitored them throughout deployment.
- We developed a plan for halting rollout in case demand outpaced capacity.

We deployed the program on a site-by-site basis, starting in the United States and continuing in other geographic regions. We scheduled communication with employees at each site about three weeks before program launch, using tools such as newsletters and the handheld social media community to set expectations. Initial communications announced program launch, provided a schedule, and discussed program eligibility and the service agreement. Communications closer to the launch date announced that employees could begin ordering service.

Historically, IT has been responsible for providing and configuring new devices. With the personal device program, the service ordering process is automated—once employees' managers provide approval, the back-end configurations occur and configuration instructions are sent directly to employees. The instructions are sent over the air, allowing employees to configure their own devices.

Best Practice #8: Stay Up to Date with Changing Technology

Technology changes at a rapid rate. It is important that we keep pace with these changes and how they affect the integration of personal devices into the enterprise.

- **Modify the service agreements as necessary.** The service agreements for personal devices were written broadly to minimize future changes. We review the service agreements every six months and modify them as necessary to reflect new technology or developing concerns. For example, with the release of a new device that enabled a personal hot spot feature, we needed to refresh a service agreement to address additional security concerns as well as the new use case of employees providing connectivity services to other employees.
- **Simplify the Web portal.** Adding personal devices to the handheld Web portal made it much more complex. Over time, we anticipate re-designing and re-organizing the Web portal to streamline the information available there.
- **Certify new OSs.** As new consumer devices come to market, employees hear about them and want to use them. Intel IT needs to respond quickly to employee requests by signaling our intentions and implementing support as appropriate. To achieve this, we provide positioning statements that indicate which OSs and devices we plan to support, and when we anticipate supporting them. Whenever possible, we provide this statement soon after products are announced and before they become available. This enables employees to anticipate our plans before they decide to buy specific devices. We also aim to support new devices or OSs as soon as it is feasible to do so; in some cases, we have added a device to our program on the first day it became available.
- **Add new services.** Currently, we offer e-mail, contacts, and calendar services on personal devices. But as security features on devices mature and we allow them to connect to the Intel Wi-Fi network, we anticipate enabling additional services. Also, we are investigating re-architecting certain services, such as the applications for scheduling an airport shuttle or submitting expense reports, so that they do not require access to the Intel intranet.
- **Deploy alternative form factors.** We envision enabling the use of alternative form factors in the future, such as televisions and devices controlled through gestures.

Because the consumer device marketplace is so dynamic, we have found new ways for our organization to be more nimble in turn. For example, as we discuss with other companies how they are integrating personal devices into their own enterprises, we have learned new things and have subsequently evaluated whether we can use those ideas to improve our personal device program.

RESULTS

Implementing personal devices has resulted in significant benefits to both program participants and to IT.

- **Increased productivity.** Employees who use personal devices report saving 47 minutes per day on average—about 10 percent of an eight-hour workday. This adds up to total time savings of 1.7 million hours per quarter. Surveys that included data from both corporate and personal devices yielded similar results—an average time savings of 57 minutes per day.
- **Improved flexibility.** Employees send approximately 2.68 million business-related e-mail messages each quarter from corporate and personal devices.
- **A high level of employee satisfaction.** The satisfaction rate exceeds 94 percent among employees using personally owned devices.
- **Relatively low cost to Intel IT.** Analysis shows that carrier service plans account for most of the total cost associated with handheld devices. With personal devices, employees pay for the device and the service plan, so the cost of enabling new devices in our environment is low. Because we support the same OSs for both corporate and personal devices, the personal device program does not affect the cost of introducing a new OS or OS version.
- **No impact on support.** The number of Service Desk tickets related to handheld devices has not increased significantly, despite the addition of 15,000 personal devices in our environment. Averaged across all corporate and personal devices, the number of tickets per user has actually decreased.
- **Enhanced business continuity.** If employees' mobile business PCs are temporarily nonfunctional, personal handheld devices provide partial backup and access to a limited number of tools—enabling employees to accomplish some tasks until their PCs are repaired.
- **Greater security and loss prevention.** Our personal device program provides a secure and managed way for employees to use their personal devices, which protects Intel data. Internal incident data indicates that employees tend to take better care of their own belongings and lose personal devices less frequently than corporate-owned devices—also enhancing information security.

CONCLUSION

Because IT consumerization is not a passing trend, Intel IT took a proactive approach to enabling personal devices in the enterprise in a secure manner—achieving the benefits of increased employee productivity, flexibility, and job satisfaction as well as enhanced security at low cost to Intel.

Our goal is to provide greater productivity and flexibility for our employees by enabling a seamless, consistent experience across devices while protecting enterprise data. We anticipate that our continued efforts to implement Intel's vision of the Compute Continuum will result in significant benefits for employees and for Intel. We currently support five major mobile OSs and have established a certification process that enables us to quickly support new product releases.

Based on our experience establishing a personal device program, we developed a set of best practices:

- Identify and engage stakeholders early in the planning process
- Engage end users
- Develop a security model
- Decide which devices to implement
- Address legal and human resources concerns
- Enable the technology
- Plan the deployment
- Stay up to date with changing technology

We have already realized measurable productivity benefits from supporting personal handheld devices. In a recent survey, employees reported saving almost an hour per day by using smart phones to access e-mail and other corporate services. In the future, we plan to support even more form factors and expand the services available to handheld devices.

FOR MORE INFORMATION

Visit www.intel.com/IT for white papers on related topics:

- "Benefits of Enabling Personal Handheld Devices in the Enterprise"
- "Maintaining Information Security while Allowing Personal Hand-Held Devices in the Enterprise"
- "The Future of Enterprise Computing: Preparing for the Compute Continuum"
- "Preparing the Enterprise for Alternative Form Factors"
- "A Roadmap for Connecting Smart Phones to the Intel Wi-Fi* Network"
- "Cloud Computing: How Client Devices Affect the User Experience"

CONTRIBUTORS

Kevin Breen, Handheld Service Line Manager, Intel IT

Mary Connaire, Handheld Engineering Manager, Intel IT

Paul Donohue, Handheld Client Engineer, Intel IT

Derek Harkin, Handheld Client Engineer, Intel IT

Ian Soanes, Handheld Product Manager, Intel IT

ACRONYMS

EOL	end of life
EULA	end user license agreement
FAQ	frequently asked question
GPS	global positioning system
HR	human resources
IDS	Intrusion Detection System
ROI	return on investment
TCO	total cost of ownership
VoIP	Voice over IP

For more information on Intel IT best practices, visit www.intel.com/it.

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 patent, copyright, or other intellectual property rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Printed in USA
1211/JLG/KC/PDF

♻ Please Recycle
326521-001US