How to Effectively Manage Your Organization's Mobile PCs

*Practical Advice from the Microsoft® Field*

Written with advice from Steve Campbell and Doug Davis

Published: April 2007



**Executive Summary**

Mobile PCs unleash productivity and bring agility to organizations by enabling a mobile workforce. However, for many organizations, deploying and managing mobile PCs can be a challenge. In this white paper, Steve Campbell and Doug Davis, Architects at Microsoft Services, share their recommendations for effectively reducing the cost and complexity of mobile PC deployment and management.



# Overview

The use of mobile PCs (laptop PCs and Tablet PCs) is a growing trend for enterprise and mid-sized organizations. In North America and Western Europe, 2010 will be a turning point at which most hardware shipments will be mobile PCs. Enterprises are enabling their mobile workforces to increase their productivity, reduce customer response time, and gain a competitive advantage. According to Gartner, Inc., “Mobility is important to the CIOs we surveyed. Not only is it ranked third in their technology initiatives, but mobility spending growth (at 3.6%) is well ahead of IT budget growth, which averages 2.7% globally”[[1]](#footnote-2).

While mobile PCs are increasingly more critical to enterprise strategy and success, their use introduces unique challenges. Deploying and managing mobile PCs is perceived as costly and time consuming, and mobile PCs raise new issues around security and productivity of mobile workers. Some of the common questions asked by businesses include:

**Deployment:** How can we easily deploy mobile PCs?

**Manageability:** How can we reduce the support associated with mobile users, and how do we keep mobile PCs updated?

**Security:** How can we protect sensitive data when the data leaves the office, and how do we keep malware from coming back into the office?

**Productivity:**  How can we facilitate productivity outside the office while attracting workers with a flexible work environment, and how can we reduce the IT burdens on remote workers?

This white paper helps answer these questions by describing the experiences and highlighting recommendations from Microsoft Services Architects Steve Campbell and Doug Davis (profiles below), who have experience effectively deploying and managing mobile PCs.

Although much of the guidance in this white paper applies to both Windows® XP and Windows Vista™, we will discuss Windows Vista in more detail, because it significantly improves the enterprise mobile PC experience. Using Windows Vista, enterprises can more easily deploy mobile PCs, and keep them running smoothly and more securely with less Information Technology (IT) support. The Windows Vista operating system has multiple layers of security to help protect mobile PC users from malicious software (also called *malware*), data theft, and other threats. Mobile PCs running Windows Vista make it easier to be responsive, communicate, and accomplish tasks in a wide variety of locations away from the office. Mobile PCs running Windows Vista give mobile workers the ability to collaborate, communicate, and get information quickly from anywhere.

**Contents**

* Deployment Guidance (pages 4–8)
* Manageability Guidance (pages 9–12)
* Security Guidance (pages 13–17)
* Productivity Guidance (pages 18–20)

## More about the authors

## Steve Campbell

Steve Campbell is an Architect at Microsoft Services. He focuses on deployment and provisioning solutions. Based in Nashville, Tennessee, Steve has been involved in the development and delivery of deployment solutions and best practices for six years. He works closely with Redmond-based product and solution accelerator teams in development, testing, training, and documentation of Microsoft deployment technologies, including Business Desktop Deployment (BDD) 2007 for Windows Vista and the 2007 Microsoft Office*®* system, the Application Compatibility Toolkit (ACT), the Microsoft® Windows User State Migration Tool (USMT), and Microsoft Systems Management Server (SMS) 2003.

Steve is also heavily involved in the development and training of both Microsoft Services and partner resources in the areas of deployment and provisioning, including the Accelerated Desktop Deployment Program (ADDP) and Desktop Deployment Planning Services (DDPS). Steve contributes to deployment-related articles for Microsoft TechNet and TechNet magazine. He speaks frequently at TechEd, Microsoft Management Summit (MMS), IT Forum, and deployment-focused events for Microsoft.

Steve has worked with over 50 organizations, from 1,500 seats to 150,000 seats. His engagements range from desktop deployment design and implementation to SMS 2003 design and implementation. He is currently working with multiple Fortune 100 companies and branches of the U.S. government and military on Windows Vista readiness and deployment recommendations.

## Doug Davis

Doug Davis is a Lead Architect at Microsoft Services. He focuses on management and deployment solutions. Doug has been involved in the development and delivery of deployment solutions and best practices, including working closely with Redmond-based product and solution accelerator teams in the development, testing, training, and documentation of Microsoft deployment technologies, including BDD 2007, Microsoft Operations Manager (MOM), and SMS 2003. Doug has B.S. degrees in Computer Science and Information Systems. He has a Masters degree in Management Information Systems.

Doug has helped more than 100 companies (from a few hundred seats to over 150,000 seats) deploy Windows XP since 2001, and has helped more than 20 companies with Windows Vista deployments. Engagements have ranged from desktop deployment design and implementation to Zero Touch Installation (ZTI) using SMS 2003. He is currently helping companies with Windows Vista readiness, deployment, and management.

# Deployment

Organizations sometimes delay the deployment of a new operating system version to their mobile PCs because upgrades can be perceived as expensive and time consuming. Mobile PC purchases tend to result in a heterogeneous environment, which requires more images to support. The effort required to support images (including development, test, and maintenance) adds significant costs to mobile PC ownership. Furthermore, resources spent maintaining images are not available to support strategic, higher-value tasks.

Some organizations have overcome these challenges by implementing the following recommendations, which the subsequent sections describe in more detail.

## Recommendation Highlights

* 1. Reduce Image Count.Significantly reduce the number of images you maintain and deploy by using the tools, technologies, and best practices that Microsoft provides.
  2. Reduce Shipping Costs.Use removable media to deploy operating system images and save shipping costs. Alternatively, you can deploy images during field meetings.
  3. Reduce Management Costs.Move mobile PCs from an unknown and unmanaged state to a known and managed state. Computers in a known state are easier and less expensive to manage.
  4. Track Assets Accurately.Use volume activation, Microsoft Asset Inventory Service, Microsoft Systems Management Server (SMS) 2003, or System Center Configuration Manager (SCCM) 2007 to track software assets and licensing.

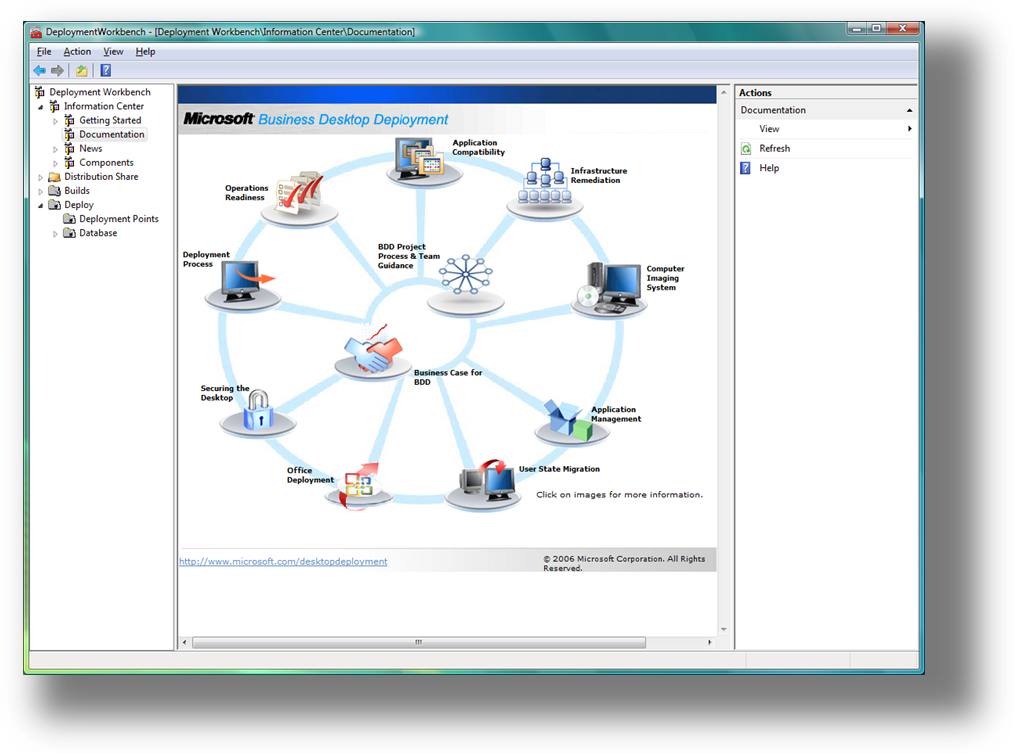
Recommendation Details

### 1. Reduce Image Count

According to Microsoft and industry analysts, a key way an organization can reduce mobile PC deployment costs is by reducing the number of images it builds and maintains. Microsoft recommends several methods for reducing the image count in your organization:

* Leverage the Image Management Features in Windows Vista.Windows Vista ultimately helps you reduce image count—even when deploying the operating system to heterogeneous mobile PCs. New features and technologies, such as a single worldwide binary, hardware independence, offline servicing, and improved deployment tools make reducing mobile PC images to just one or two more possible and less expensive than in earlier versions of Windows. For example, rather than building one image for each language, you can eliminate the costs of additional images by building a single language-agnostic image. Doug Davis, Lead Architect at Microsoft Services, explains, “We don’t integrate language packs in to the core image. We detect the language during deployment and add it dynamically.” Rather than recreating an image to add an update or device driver, quickly add the update to an image offline, and eliminate the time required to redevelop and retest the image. Windows Vista also simplifies Tablet PC deployment. It supports Tablet PCs natively, without requiring components from additional media.
* Use BDD 2007 Best Practices and Guidance.Microsoft recommends that you use BDD 2007 (**Figure 1**) to deploy Windows Vista to mobile PCs. According to Steve Campbell, Architect at Microsoft Services, “BDD is the single best way you can reduce the number of images you build and maintain and reduce other costs associated with mobile PC deployment.” BDD 2007 provides the guidance and framework that help you more efficiently deploy the operating system to mobile PCs. It fully leverages the latest deployment technology from Microsoft, including the new version of the System Preparation Tool (SysPrep), the Microsoft Windows Automated Installation Kit (Windows AIK), and the Windows Preinstallation Environment (Windows PE). Customers can also significantly reduce costs by using System Center technologies, enabling zero-touch deployments based on BDD methodology. BDD 2007 supports nondestructive imaging and removable media, so you can deploy Windows Vista to mobile PCs by using removable media instead of requiring mobile users to ship or bring in their computers to the office. Significantly, BDD 2007 allows you to install device drivers and applications based on the mobile PC model, so you can deploy a single image to a variety of mobile PC models, and then install original equipment manufacturer (OEM) applications and device drivers specific to the make and model of the computer. For more information about using BDD 2007, see Microsoft Solution Accelerator for Business Desktop Deployment 2007 at <http://www.microsoft.com/desktopdeployment>.

**Figure 1**



*“BDD is the single best way you can reduce the number of images you build and maintain and reduce other costs associated with mobile PC deployment.”*

– Steve Campbell

* Reduce Hardware-Specific Configuration Dependencies. Application dependencies include authentication mechanisms, dialers, virtual private network (VPN) clients, and OEM applications. You can reduce application dependencies by deploying *thin images* (basic images that are customized post-deployment), and then installing applications based on role or mobile PC model after deployment. Doug says, “We look up the device type during deployment and install applications and device drivers just-in-time instead of trying to integrate them in to the image. We have really thin images with no or very few applications.”
* Standardize Your Hardware. Even though Windows Vista provides hardware-agnostic technologies, homogeneous environments still have lower development, test, deployment, and support costs than heterogeneous environments.

### 2. Reduce Shipping Costs

*“Getting your deployment cost down to $100 is really difficult when it costs $50 to ship the mobile PC to and from the office”*

– Doug Davis

Another way you can reduce deployment costs is by using removable media (DVD, USB Flash disk, removable USB hard drives, and so on) to install images. According to Doug, “Getting your deployment cost down to $100 is really difficult when it costs $50 to ship the mobile PC to and from the office. And it’s difficult to put a value on the time mobile users lose while waiting for their mobile PCs.” He suggests the following options for handling mobile PC deployment logistics:

* Deploy by Using Removable Media. BDD 2007 makes removable media-based deployment possible in mobile PC scenarios, so mobile PCs don’t have to have a connection to the corporate network to install the latest image. Doug says, “We’ve created solutions on 4 GB removable drives that save the user’s documents and settings locally, re-image the mobile PC, reinstall the user’s applications, then restore the user’s documents and settings—automatically, every time the user plugs in the drive.” The nondestructive nature of Windows imaging makes this possible. For more information on the nondestructive nature of Windows imaging, visit <http://technet.microsoft.com/en-us/windowsvista/aa905116.aspx>.
* Deploy During Field Meetings.Deploy images to all your mobile PCs during annual meetings, sales retreats, or other gatherings. This requires that you set up a temporary deployment depot at the meeting, but it simplifies support challenges by minimizing configuration variations.

### 3. Reduce Management Costs

According to Doug Davis, “Our preferred practice is to do a wipe-and-load to get mobile PCs back to a known, consistent, and standardized state. The challenge is getting users’ applications, documents, and settings back to where they were without carrying forward unwanted applications and settings.” Microsoft recommends that you take the following steps to prepare for better management of mobile PCs:

* Wipe-and-Load Mobile PCs Rather Than Upgrading Them in Place. “From a corporate risk and reliability standpoint, the best thing you can do is reset mobile PCs to a known state,” says Doug. To reset mobile PCs, you must wipe-and-load them with a new operating system image rather than upgrading to the operating system in place. This in-place wipe-and-load is possible by the nondestructive nature of Windows imaging available in Windows Vista.
* Use the User State Migration Tool (USMT) to Migrate Documents and Settings. Mobile PCs are different from desktop PCs in that all data and settings reside on the mobile PC. Users’ critical data is often on their mobile PCs only and not replicated to corporate file servers. They don’t always have access to network shares. They aren’t using folder redirection or offline files. Regardless, BDD 2007 uses USMT to store users’ documents and settings on the local hard disk and then restore them after installing a new image on the mobile PC. This helps you reset the mobile PC to a known, manageable state without sacrificing mobile user’s productivity.
* Repackage Applications and Engineer Images So That They Install Silently. If mobile users must interact with setup programs during installation, you cannot guarantee configurations will be standardized and consistent across all mobile PCs. Therefore, Microsoft recommends that you repackage applications so they install silently. According to Doug, “You should create a fully automated deployment process, preventing users from creating one-off configurations that are difficult to support.” BDD 2007 includes guidance for fully automating installation, including how to repackage applications.

### 4. Track Assets Accurately

Lack of asset tracking is often a deployment roadblock. Organizations simply don’t know absolutely what hardware and software is in their inventory, and who owns them. They don’t know where equipment goes after release. They also don’t have a way to track license compliance, and they don’t know have a way to target specific mobile PCs and users for deployment. Microsoft recommends that you use the following tools and technologies to help better track assets in your organization:

* **Use Volume Activation to Control Windows Vista Licensing.** Volume activation is a new Windows Vista technology that helps you protect your volume license keys and prevent over- and under-licensing. Volume Activation 2.0 provides customers with the following two types of keys and three methods of activation – Multiple Activation Key (MAK) and Key Management Service (KMS) key.

Using MAK, each product key can activate a specific number of computers. If the use of volume-licensed media is not controlled, excessive activations result in depletion of the activation pool. MAKs are activation keys. They are not used to install Windows but rather to activate it after installation. You can use them to activate any volume edition of Windows Vista.

KMS enables organizations to perform local activations for computers in a managed environment without each computer individually connecting to Microsoft. A KMS key is used to enable the Key Management Service on a computer controlled by an organization’s system administrator. KMS use is targeted at managed environments where more than 25 computers are consistently connected to the organization’s network. Computers running Windows Vista activate by connecting to a central Windows Vista computer running the KMS service. (Learn more about volume activation from Windows Vista Volume Activation 2.0 Technical Guidance at <http://www.microsoft.com/technet/windowsvista/plan/volact.mspx>.)

MAK activation keys activate once, directly to Microsoft, so they are appropriate for mobile PCs that connect infrequently to the corporate network. If you use MAKs for mobile PCs and KMS keys for desktop PCs, you create a situation in which you must create an image for each product key. According to Doug, “The best practice is to use the BDD 2007 OverrideProductKey property to override the KMS key in an image with a MAK.” This way, you can deploy an image containing a KMS key to mobile PCs, and then make a just-in-time decision to override the key with a MAK. Well-connected mobile PCs can use KMS keys, assuming they connect to the corporate network regularly.

* **Use the Microsoft Asset Inventory Service.** Part of the Microsoft Desktop Optimization Pack for Software Assurance, the Microsoft Asset Inventory Service provides an intelligent and comprehensive view of your enterprise’s desktop software inventory. It helps you effectively manage your software asset inventory to ensure compliance and optimize your IT budget. It also helps reduce application deployment costs, enable delivery of applications as services, and enable better management of your mobile PCs. This service is expected to be available by fall 2007.
* **Deploy Systems Management Server (SMS) 2003 or System Center Configuration Manager (SCCM) 2007.** SMS 2003 and SCCM 2007 provide rich inventory and use-tracking features that help reduce application deployment costs and help you track your software asset inventory. Both tools enable simplified license compliance tracking by monitoring concurrent application use, providing you with the information you need to make informed licensing decisions.

**Fujitsu Consulting**

Fujitsu Consulting has a growing mobile workforce and has a track record of controlling information technology (IT) costs. The company is improving their track record even further by using these best practices and technologies. Instead of maintaining 15 operating-system images, Fujitsu Consulting is building just one or two images for their mobile PCs. Mahesh Punyamurthula, Lead for the Windows Vista Application Compatibility Project, says the company expects to reduce the time that IT spends building and maintaining images by 30 to 35 percent. For more information about this study, go to <http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=201143>.

# Manageability

By nature, mobile PCs are more difficult to manage than desktop PCs, because they don’t connect to corporate networks as frequently as desktop PCs and are not physically accessible by IT. “The problem is that managing mobile PCs consistently or effectively is difficult if they don’t connect to the corporate network regularly,” says Steve Campbell, Architect at Microsoft Services. “Mobile PCs that connect infrequently present a security risk when they come back on-site, unless you’re able to quarantine them. And when they do come back on-site, they get bogged down catching up with security updates.” As a result, the key to managing mobile PCs is to ensure that they connect to the network frequently.

You can manage mobile PCs more effectively by ensuring your mobile PCs consistently connect to the corporate network, and then applying Group Policy to them. Microsoft recommends you take the following steps to successfully manage your mobile PCs, which are described in more detail in the following sections.

## Recommendation Highlights

1. Connect Mobile PCs to the Network. Ensure that mobile PCs connect to the corporate network regularly (at least monthly), so that you can effectively manage them by using your existing management infrastructure (for example, Group Policy).
2. Use Group Policy to Manage Settings. By using Group Policy to manage settings, you can enforce a standard, well-known configuration that ensures the security of your assets and corporate network.
3. Encourage Mobile Workers to Use Network Diagnostics. Teach mobile users how to diagnose and resolve network connection issues.
4. **Provide Remote Assistance.** Enable and properly configure Remote Assistance on mobile PCs.

## Recommendation Details

### 1. Connect Mobile PCs to the Network

Microsoft suggests the following steps for connecting mobile PCs to the corporate network regularly:

* Configure the Native VPN Client to Connect to Your Network.VPN connections provide a more secure, reliable connection to the corporate network through any Internet connection. They allow organizations to get more information (policies, virus scans, inventory updates, and patches) to mobile PCs more often. Windows Vista includes a native VPN client you can configure to connect to the corporate network. The native client supports Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP)/IP Security (IPSec). For more information about the Windows Vista native VPN client, see Virtual Private Networks at <http://www.microsoft.com/technet/network/vpn/default.mspx>. Alternatively, you can deploy a third-party VPN solution.
* Teach Mobile Users to Connect to the Network Frequently. Communicate regularly with mobile users about the importance of connecting to the corporate network. When mobile users don’t frequently connect to the corporate network, their mobile PCs are at risk. When they do connect to the network, it might take a significant amount of time to update them. “Connecting once a week is ideal, and once a month should be the minimum frequency,” according to Steve.

*“Connecting (to corporate network) once a week is ideal, and once a month should be the minimum frequency”*

– Steve Campbell

* Expose Field Tools Through the Corporate Extranet. Microsoft recommends that you make mission-critical field tools, such as Customer Relationship Management (CRM) tools, available to mobile users through the extranet by using technologies such as Remote Procedure Call (RPC) over Hypertext Transfer Protocol (HTTP). For example, you can create an Internet-facing Web site that mobile users can use to update their mobile PCs. You can configure Microsoft Office Outlook® 2007 to use RPC over HTTP to connect to a computer running Microsoft Exchange Server without first establishing a VPN connection. In the future, you will be able to use Microsoft System Center Configuration Manager (SCCM) 2007 to manage mobile PCs through the Internet.
* Use Multifactor Authentication to Protect VPN Connections. Use a combination of smartcards and credentials to protect access to network connections. Doing so helps to secure access to resources on the corporate network while allowing easy access for legitimate mobile users.

### 2. Use Group Policy to Manage Settings

Group Policy is an efficient and effective management technology that most organizations already use. Microsoft makes the following recommendations for using Group Policy to manage mobile PCs:

* Review the Group Policy Scenarios White Paper. The white paper “Group Policy Common Scenarios Using GPMC” at <http://www.microsoft.com/downloads/details.aspx?familyid=354B9F45-8AA6-4775-9208-C681A7043292&displaylang=en> contains a sample scenario for mobile PCs. Review this scenario to better understand how you can use Group Policy to manage your mobile PCs.
* Review the Group Policy Settings Reference. The Group Policy Settings Reference is a spreadsheet that describes available Group Policy settings, including mobile PC settings such as removable storage management and wireless network configuration. This spreadsheet provides a complete inventory of Group Policy settings that you can evaluate. Review this reference to determine which policies are most appropriate for the mobile PCs in your environment. Two versions of this reference are available:
* Windows XP at <http://www.microsoft.com/downloads/details.aspx?familyid=7821C32F-DA15-438D-8E48-45915CD2BC14&displaylang=en>
* Windows Vista at <http://www.microsoft.com/downloads/details.aspx?familyid=41dc179b-3328-4350-ade1-c0d9289f09ef&displaylang=en>
* Document Security Policies, and Then Enforce Them by Using Group Policy. Each organization is different. However, you can easily discover the policies you must configure in your organization. First, examine regulatory requirements with which you must comply. Also, interview key stakeholders to determine their requirements. Document these policies and communicate them to your mobile users. After discovering and documenting your policies, use Group Policy to enforce them.
* Extend the Windows Server 2003*®* Active Directory Schema to Manage Windows Vista Wireless Networking. Windows Vista supports enhanced management of wireless networking connections, giving you greater control of which wireless connections can be used by mobile PCs. Before you can use these features, however, you must extend the Windows Server 2003 Active Directory® directory service schema. For more information, see Active Directory Schema Extensions for Windows Vista Wireless and Wired Group Policy Enhancements at <http://www.microsoft.com/technet/network/wifi/vista_ad_ext.mspx>.

### **3. Encourage Mobile Workers to Use Built-in Diagnostics**

### Windows Vista puts you in control of your network experience with the Network and Sharing Center, where you can check your connection status, see your network visually, or troubleshoot a connection problem. The Network and Sharing Center informs you about the network your computer is connected to and verifies whether it can successfully reach the Internet. It even presents this information in a summary form called the Network Map so you can immediately see your connectivity to the network and to the Internet. If a computer on the network loses Internet connectivity, you can graphically see which connection is down and then use Network Diagnostics to help determine the cause of the problem and find possible solutions.

### The built-in performance diagnostics in Windows Vista can detect and self-correct many performance issues. Performance diagnostics provide instrumentation and services for both user-driven and tool-driven diagnoses of common problems, including rough media playback, slow application startup, slow startup of the operating system, and network-related delays. Built-in performance diagnostic tools track how long it takes to execute common activities, analyze performance declines, and display results in the Performance Center, where users can then take action to remedy the problem. Performance issues are also written to the system event log, where they can be monitored by users or by support professionals.

### Windows Vista also includes new tools and instrumentation that make it easier for IT administrators to manage system performance. For example, performance counters are more widely implemented, reliable, and secure. For IT professionals, a new performance monitor snap-in to the Microsoft Management Console provides a better user experience and allows easier monitoring and diagnoses of performance-related issues.

### 4. Provide Remote Assistance

### Mobile users are disconnected from the corporate network and, as a result, more difficult to support. Microsoft suggests that you enable and properly configure Remote Assistance—a tool built into Windows that you can use to provide remote help. You must configure Remote Assistance by using Group Policy to define the accounts that can provide remote assistance. You must also configure Group Policy to allow the Remote Assistance program to pass through the firewall, which limits the attack surface of Remote Assistance. By configuring Remote Assistance using Group Policy, support technicians can invite themselves to provide help without requiring the mobile user to initiate it.

**The University of Pittsburgh Medical Center**

The University of Pittsburgh Medical Center (UPMC) is the premier health system in western Pennsylvania and one of the most renowned academic medical centers in the United States. UPMC has approximately 30,000 workstations for its 40,000 employees, 5 percent of whom are mobile workers. Says Ryan Harvey, Project Manager of Desktop Design, “We wanted a more manageable client infrastructure, in which we could make security-related changes and updates more easily and configure the computers at a more detailed level—without compromising our users’ productivity.” Windows Vista will help UPMC manage its infrastructure more completely and effectively. “Overall, the upgrade will give us the ability to better manage our environment,” says Ward Miller, System Analyst. “All the configuration options in this operating system are addressable through Group Policy, so we’ll be able to be much more granular in our approach to controlling the environment.” The organization anticipates that having a more controlled environment will result in a decrease in the volume of help-desk calls. For more information about this case study, go to <http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=201057>.

# Security

Mobile PCs are more prone to theft and loss than desktop PCs, simply by the fact that they leave the office. After mobile PCs are lost or stolen, the organizations’ intellectual property, including proposals, specifications, and even sensitive customer information is at risk. Organizations strive to ensure that their intellectual property and customer data are safe to protect against legal noncompliance, financial loss, and loss of credibility.

Additionally, some governments are passing security breach notification laws. In the United States, more than 30 states have passed statutes that require organizations to notify consumers in the event of accidental or illicit data disclosure. Besides these state regulations, national and regional regulations provide similar restrictions and penalties, including HIPPA, GLBA, SOX in the U.S., PIPEDA and PHIPA in Canada, European Data Protection Directive in the European Union, DPA in the UK, and APECTEL in Asia Pacific[[2]](#footnote-3).

In the following sections we outline some of the major security challenges and best practices in managing technologies to help overcome these challenges.

* **Security Risks of Logging on as Administrator.** In the past, Windows XP users were frustrated by the limitation of standard user’s rights for completing even simple tasks, such as changing the time zone while traveling. As a result, organizations tended to grant mobile users Administrator rights. In turn, these users with administrative privilege would accidentally install malware (and then bring it into the corporate environment) or inadvertently change settings that can compromise the security and stability of the system.
* **Spyware.** Over the past several years, spyware and other malicious software have caused major problems for computer users. The recent upsurge in spyware has largely been driven by the business opportunity to generate income from spyware distribution. Unwanted spyware is found on more than two-thirds of all computers, and is putting users’ privacy and personal information at risk, as well as causing significant performance and reliability issues.
* **Security updates.** Mobile PCs are more difficult to keep updated and secure than desktop PCs, because they aren’t persistently connected to the corporate network. This is exacerbated by the fact that mobile PCs are more exposed to malware because they connect to large numbers of remote networks that are beyond their organization’s control, including airport kiosks, hotel lobbies, and coffee shops. Infected mobile PCs bringing malware back to the corporate network and infecting other computers is a substantial risk.

For most organizations without Windows Vista, maintaining the security of their mobile PCs is a race. IT divisions are constantly maintaining virus-detection agents, updating definitions, and configuring firewalls—all last lines of defense, susceptible to change if users log in as Administrators. In fact, much of the money IT spends is focused at these tasks as well as on securing messaging systems.

To achieve higher levels of mobile PC security, Steve recommends that you take the following steps.

## Recommendation Highlights

1. Protect Corporate Data From Theft. Use the best available data encryption technologies to help protect intellectual property, including customer information, to help keep data is safe even if the mobile PC is stolen.
2. Ensure Users Log on as Standard Users. Use the features available for preventing users from accidentally installing malware or making undesirable changes to their mobile PC configurations.
3. Keep Mobile PCs Current with Security Updates. Keep the security updates on mobile PCs current so that those computers don’t bring threats back in to the network and don’t bog down when they install updates. Consider checking the health of your mobile PCs before you allow them access to the domain.
4. Help Secure Mobile PCs from Malware. Help mobile users remain savvy to security threats by using Windows Security Center to update them when their mobile PCs are at risk.

For more information about Windows Vista security, see **Windows Vista Security Guide** (<http://www.microsoft.com/technet/windowsvista/security/guide.mspx>) and **Data Encryption Toolkit for Mobile PCs** (<http://www.microsoft.com/det>).

Recommendation Details

### 1. Protect Corporate Assets from Theft

Both Windows XP and Windows Vista provide features that you can leverage to help protect intellectual property even if a mobile PC is lost. Microsoft recommends that you take the following steps to access those features:

* Deploy Windows Vista Enterprise to Take Advantage of Windows*®* BitLocker™ Drive Encryption with the Trusted Platform Module (TPM). Windows Vista Enterprise and Windows Vista Ultimate provide full-volume encryption that goes beyond Encrypting File Service (EFS). Users tend to store data in various locations, not just in their My Documents folder. Windows*®* BitLocker Drive Encryption protects this data by encrypting the entire volume rather than individual folders. It also protects data that applications might cache in various locations, such as in the Temporary folder. You can easily manage the encryption by using Active Directory and Group Policy. For example, you can store encryption keys in Active Directory, providing data recovery without using new or redundant infrastructure. Also, using BDD 2007 you can easily configure BitLocker Drive Encryption during deployment. Windows*®* BitLocker works ideally on the computer hosting the TPM. You might consider a multifactor pre-boot authentication option for BitLocker for your users who have intellectual property data on their computers. If you decide to implement multifactor TPM plus PIN, it is much easier to manage than TPM plus USB device.
* Take Advantage of Active Directory to Facilitate the Key Recovery Process in Using Windows*®* BitLocker Drive Encryption. Steve Campbell, Architect at Microsoft Services, says, “To help your BitLocker Drive Encryption deployment, be mindful to prepare the help desk for key recovery.” This allows you to recover mobile users’ data in the event that they cannot start or access their computers. You should also extend the Active Directory schema to store BitLocker Drive Encryption keys for recovery purposes. For more information, see Configuring Active Directory to Back up Windows BitLocker Drive Encryption and Trusted Platform Module Recovery Information at <http://technet2.microsoft.com/WindowsVista/en/library/3dbad515-5a32-4330-ad6f-d1fb6dfcdd411033.mspx?mfr=true>.
* Implement the Encrypting File System (EFS). EFS requires no additional hardware or software, and it works on all mobile PCs that are running business-oriented Windows versions[[3]](#footnote-4). Organizations with Active Directory can turn on Folder Redirection, make users’ data available offline, and then use EFS to encrypt that data. Using EFS provides basic data security, and you can manage it by using Group Policy. Using Windows Vista, you have the added benefit of encrypting swap files and obtaining better protection of Windows directory, page file, and deleted temporary files.
* If You Are Considering a Rollout, Start with the Mobile Users According to the Sensitivity of Data They Use. You should require mobile PCs containing personal data to have TPM chips and use BitLocker Drive Encryption to encrypt the whole volume, though. Doug Davis, Lead Architect at Microsoft Services, puts it simply: “If a mobile user works with sensitive data, then that user’s mobile PC must have BitLocker Drive Encryption no matter what, or that user simply shouldn’t be allowed to take the data outside the office.”

*“If a mobile user works with sensitive data, then that user’s mobile PC must have BitLocker Drive Encryption no matter what”*

– Doug Davis

* Review and Use the Data Encryption Toolkit for Mobile PCs. The toolkit provides guidance and tools for using EFS to protect corporate assets. For more information, see **Data Encryption Toolkit for Mobile PCs** (<http://www.microsoft.com/det>).

### 2. Ensure Users Log On as Standard Users

Microsoft Services recommends you take the following steps to balance the needs of your mobile users with the needs of the organization:

* Deploy Windows Vista Using Standard User Accounts.For Windows Vista, Microsoft redesigned commonly used features so they don’t require Administrator privileges. Doug says, “Unrestricted users (users with accounts in the local Administrators group) are a security risk, because they can accidentally install malware or make configuration changes that increase the attack surface of their mobile PC.” You can more easily deploy standard user accounts, and users can still configure common mobility settings. For example, standard user accounts can change time zones, manage printers, and change some network settings.
* In Windows XP, Control the Installation of Applications.Package applications using Microsoft Windows Installer, and use Group Policy to restrict the location from which Windows Installer packages can install. This allows mobile users to install applications, unrestricted, but only from trusted locations.

### 3. Keep Mobile PCs Current with Security Updates

To protect corporate assets and security, you must keep security updates current on mobile PCs. Some organizations don’t use Windows Update to maintain security updates, because they prefer to review and approve updates before installing them. Microsoft suggests the following methods for maintaining updates on mobile PCs:

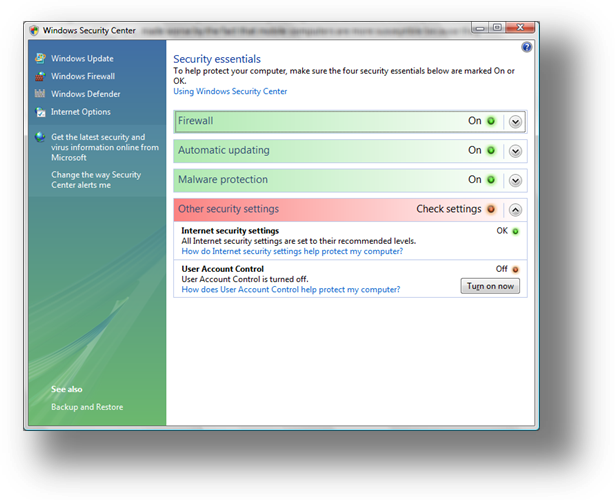
* Ensure that Mobile PCs Connect to the Network Frequently. Infrequent communication with the corporate network reduces your ability to effectively and efficiently keep mobile PCs current with the latest security updates. The section “Connect Mobile PCs to the Network” earlier in this document describes steps you can take to ensure that mobile PCs connect to the network often enough to remain current.
* Deploy Windows Server Update Services (WSUS) or SMS 2003/SCCM 2007. Using WSUS and SMS 2003/SCCM 2007, you can easily manage and deploy security updates to computers running Windows, including mobile PCs that connect frequently to the corporate network. When your mobile PCs are connecting to the network regularly, you can use WSUS or SMS 2003/SCCM 2007 to update them.
* Protect Corporate Assets. Out-of-date mobile PCs are a security risk when they come back onto the corporate network. To protect corporate assets from mobile PCs that don’t have the latest security updates, use Network Access Protection (NAP) to quarantine them until they are updated and secure. NAP requires Windows Server® code named “Longhorn.” (See Network Access Protection at <http://www.microsoft.com/technet/network/nap/default.mspx>.) Steve says that “NAP assures that only properly configured, healthy computers can connect to the network.”

### 4. Help Secure Mobile PCs from Malware

Microsoft recommends the following for securing mobile PCs from malware:

* Deploy Windows Vista, Which Is More Secure out of the Box. The behavior of Windows Vista changes depending on the type of network to which the mobile PC connects. For example, the operating system prompts for the network type (public, work, or home). Based on users’ answers, Windows Vista configures itself appropriately. If you’re using a free connection at a coffee shop, Windows Vista will disable network discovery, file sharing, public folder sharing, and so on. Windows Vista also improves upon the Windows XP firewall. The Windows Vista firewall is more manageable by Group Policy, and you can define rules for both inbound and outbound connections.

**Figure 2**



* Make Mobile Users Aware of the Windows Security Center. The Windows Security Center (**Figure 2**) monitors the mobile PC and alerts the user when security issues arise, including out-of-date virus definitions or a disabled firewall. While some organizations turn off these notifications because they think they are a nuisance or not important, they increase their risk considerably because this reduces the mobile user’s awareness.

**Avanade**

Avanade, a technology consulting leader, stays at the head of the curve by giving its consultants tools designed to increase its competitive edge. Continuing its practice of early technology adoption, the company recently upgraded to the Windows Vista operating system, Microsoft Exchange Server 2007, and the 2007 Microsoft Office system—taking advantage of expanded support for mobile workers, increased collaboration capabilities, enhanced security, and improved IT management.

Avanade has a highly mobile, distributed workforce with more than 80 percent of its employees working from outside the company’s offices. The company is using features in Windows Vista to keep information safe, such as Windows BitLocker Drive Encryption, which provides full-volume encryption and boot integrity checking to help ensure that the data on a computer stays confidential, even if the mobile PC is lost, stolen, or decommissioned. “Everyone at Avanade has a portable computer, up to and including the CEO. It could be crippling to the company if the sensitive customer data and Avanade intellectual property on any given computer were compromised,” says Josh Adams, Infrastructure Architect. “If a portable computer gets left behind, BitLocker will save the day."

For more information about this case study, go to <http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=200067>.

# Productivity

Mobile users must be self-supportive, because support is remote or not available as a result of limited connectivity. When users accidentally lose data or damage their configurations, they must be able to recover—on their own. For example, mobile users often need help recovering deleted files, or they need a way to recover those files without help. Otherwise, they are forced to redo the work they lost. Thus, a backup and restore solution is a requirement for mobile PCs.

To help keep your mobile users productive while on the road, Microsoft recommends that you take the following steps, which the subsequent sections describe in detail.

## Recommendation Highlights

1. Enable Users to Recover Data. Provide a backup and restore solution that allows mobile users to recover lost data on their own without calling the help desk.
2. Help Mobile Users Take Files Offline. Deploy Folder Redirection and Offline Files to allow mobile users to more easily take important files offline and synchronize changes when they return to the office.
3. Enable Collaboration for Mobile Users. Teach mobile users how to use the collaboration features that the Windows Vista operating system provides natively.

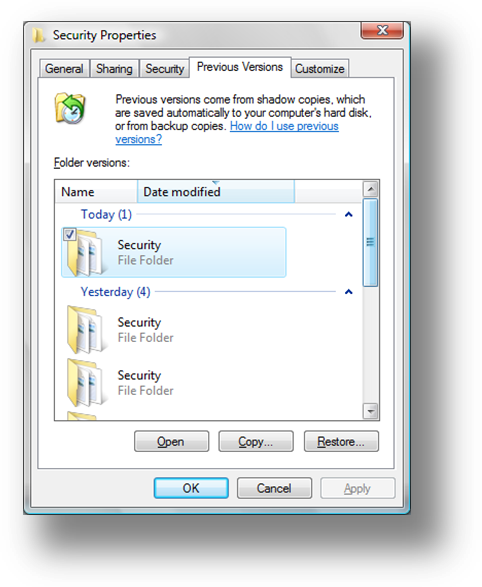
## Recommendation Details

### 1. Enable Users to Recover Data

To be self-sufficient, mobile users require tools that help them recover lost data. Microsoft recommends the following tools and technologies for helping users recover lost data:

**Figure 3**

* **Schedule Backup Jobs.** IT Administrators can use the Backup and Restore Center to create a task that enables automatic, scheduled backup of data to a second hard disk or to removable media (CD or DVD), without requiring the end user to have administrative privileges.



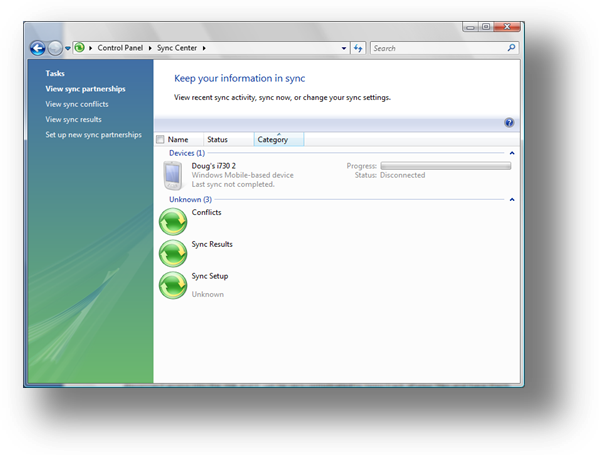
* Enable Previous Versions and Teach Users how to Use It.Using the Previous Versions tool (**Figure 3**), Windows Vista users can easily restore lost data or recover a previous version of it. For example, if a mobile user accidentally saves changes to a file, he or she can quickly and easily restore the previous version of the file. Most users don’t know about this feature, however, and so they require training. You can use Group Policy to ensure that Previous Versions is enabled in Windows Vista. Steve Campbell, Architect at Microsoft Services, adds that “making sure mobile users are using Previous Versions is a help desk thing. Rather than a call costing $90, you can make it a $25 call by teaching the mobile user how to use Previous Versions.”
* Deploy the Windows Recovery Environment (Windows RE) to Mobile PCs. Windows RE can fix many problems that prevent mobile PCs from starting at all. Steve indicates that “Windows RE can fix about 80 percent of the issues that prevent Windows Vista from starting.” For more information, see **Windows Recovery Technical Reference** at <http://technet2.microsoft.com/WindowsVista/en/library/42f74ef7-dee8-419e-989f-36b2d45c13f41033.mspx?mfr=true>.
* Purchase Rugged Mobile PCs.Hardware vendors have begun building “ruggedized” mobile PCs. Many of these computers can survive drops, and they sometimes have acceleration-detection technology that move the hard disk heads to a safe location when they anticipate a shock.

### 2. Help Mobile Users Take Files Offline

Microsoft suggests that you use the following steps to enable mobile users to take files offline when they leave the office, and then synchronize their changes when they return:

* Use Folder Redirection with Offline Files and Folders to Provide Consistent Access to Important Data.These features help mobile users be more productive whether they’re on an airplane or working at a remote site. Offline Files and Folders allow users to take any combination of files, folders, and entire mapped drives with them when they disconnect from the network. Because the feature is easy to use, you spend less time training users how to take files offline. Also, this feature is manageable through Group Policy. For example, you can configure synchronization for users and can make specific network folders available offline automatically without users needing to configure them. If you use Folder Redirection to redirect users’ My Documents folders to the network, Windows automatically makes their My Documents folder available for offline use. New features in Windows Vista help make mobile users even more productive. For example, Delta Sync allows mobile users to synchronize files more quickly by synchronizing only changes to a file and not the entire file.

**Figure 4**



* Deploy Windows Vista and Teach Mobile Users how to Use the Sync Center. The Sync Center (**Figure 4**) is a central location that allows mobile users to configure synchronization for all of their data and devices. Using the Sync Center, mobile users can also see all of their synchronization relationships in one place, and then can synchronize anytime they want.

### 3. Enable Collaboration for Mobile Users

Organizations can no longer afford for their mobile users to work in isolation. The real power of mobile computing stems from mobile users collaborating with other users—anywhere, anytime. Microsoft recommends that you deploy Windows Vista and train users how to use its collaboration features. Windows Vista provides collaboration features that help mobile users successfully work with other users, even over simple Internet protocols. For example, using Windows Meeting Space, mobile users can work face-to-face with small groups of other Windows Vista users. They can collaborate on a presentation, for example, or revise a proposal—without exchanging large, un-versioned files through e-mail.

**The Danish Tax Authority (SKAT)**

The Danish Tax Authority manages tax assessment issues, real estate evaluation, and collection of public debt, among other tax-related matters, throughout Denmark. Its 10,000 employees, who use a significant number of specialized applications and travel a considerable amount, needed a new operating system that would provide improved security, higher mobility, and simpler deployment and maintenance.

To the Danish Tax Authority, one of the crucial improvements of Windows Vista is the operating system’s Sync Center, which automatically synchronizes offline files or folders on an employee’s computer with the server when the employee returns to the office.

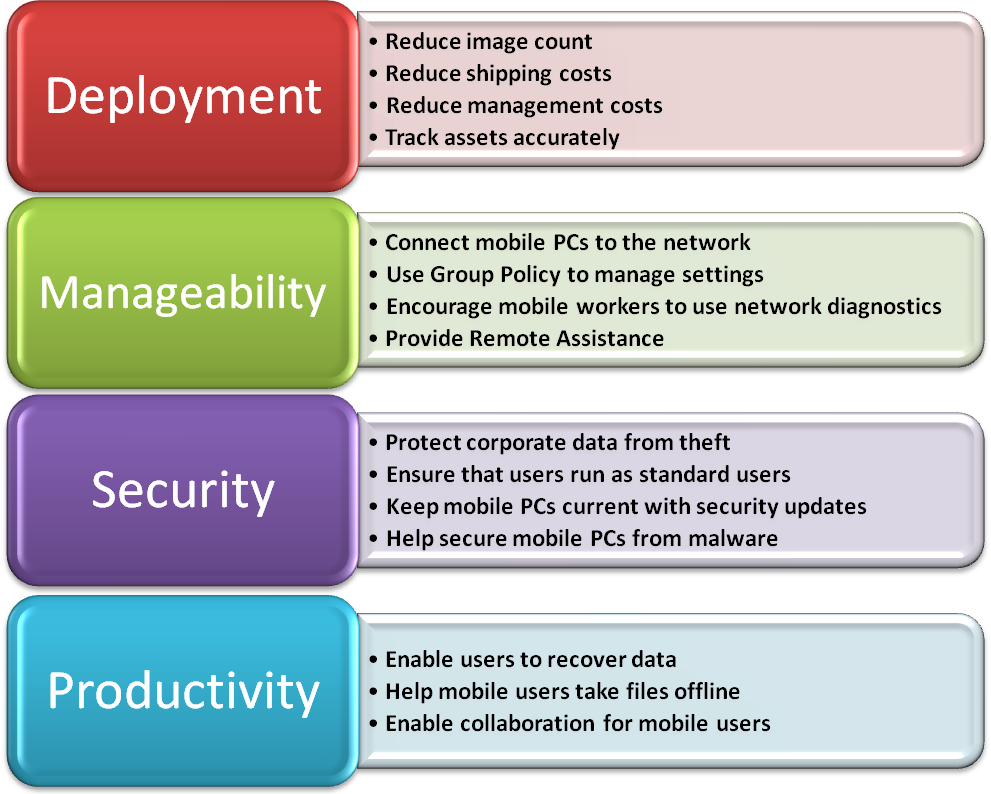
“The Sync Center is a great advantage when you work a lot with mobile units such as PDAs and mobile phones, as we do. The fact that the entire synchronization element is so closely integrated with the operating system makes it far easier to work with mobile units,” Moldt says.

For more information about this case study, see <http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=201070>.

# Summary

Mobile PCs unleash productivity and bring agility to organizations, enabling a mobile workforce. However, for many organizations deploying and managing mobile PCs can be a challenge.

In this whitepaper, we have shown you how to effectively manage your mobile PCs. The following chart (**Figure 5**) summarizes the main advice from the Microsoft field, presented as recommendations from two Architects in Microsoft Services. For more information about the recommendations in this white paper, see the section “More Information” at the end of this document.



**Figure 5**

# More Information

* Active Directory Schema Extensions for Windows Vista Wireless and Wired Group Policy Enhancements (<http://www.microsoft.com/technet/network/wifi/vista_ad_ext.mspx>)
* Configuring Active Directory to Back up Windows BitLocker Drive Encryption and Trusted Platform Module Recovery Information (<http://technet2.microsoft.com/WindowsVista/en/library/3dbad515-5a32-4330-ad6f-d1fb6dfcdd411033.mspx?mfr=true>)
* Data Encryption Toolkit for Mobile PCs (<http://www.microsoft.com/det>)
* Group Policy Common Scenarios Using GPMC (<http://www.microsoft.com/downloads/details.aspx?familyid=354B9F45-8AA6-4775-9208-C681A7043292&displaylang=en>)
* Group Policy Settings Reference for Windows Vista (<http://www.microsoft.com/downloads/details.aspx?familyid=41dc179b-3328-4350-ade1-c0d9289f09ef&displaylang=en>)
* Group Policy Settings Reference for Windows XP (<http://www.microsoft.com/downloads/details.aspx?familyid=7821C32F-DA15-438D-8E48-45915CD2BC14&displaylang=en>)
* Identity Theft at the California Office of the Attorney General Web site (<http://ag.ca.gov/idtheft/index.htm>)
* Microsoft Exchange 2000 Server Resource Kit (<http://www.microsoft.com/technet/prodtechnol/exchange/2000/library/reskit/part4/c13virus.mspx?mfr=true>)
* Microsoft Solution Accelerator for Business Desktop Deployment 2007 (<http://www.microsoft.com/technet/desktopdeployment/bdd/2007/default.mspx>)
* Network Access Protection (<http://www.microsoft.com/technet/network/nap/default.mspx>)
* Virtual Private Networks (<http://www.microsoft.com/technet/network/vpn/default.mspx>)
* Windows Recovery Technical Reference (<http://technet2.microsoft.com/WindowsVista/en/library/42f74ef7-dee8-419e-989f-36b2d45c13f41033.mspx?mfr=true>)
* Windows Vista Security Guide (<http://www.microsoft.com/technet/windowsvista/security/guide.mspx>)
* Windows Vista Volume Activation 2.0 Technical Guidance (<http://www.microsoft.com/technet/windowsvista/plan/volact.mspx>)

# Acknowledgements

Michelle Anderson, Studio B

Bill Brammer, Studio B

Carolyn Mader, Studio B

Dan Rogers, Microsoft Corporation

Hiroshi Sakakibara, Microsoft Corporation



The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2007 Microsoft Corporation. All rights reserved. Microsoft, Active Directory, BitLocker, Outlook, Windows, Windows Server, Windows Vista, and the Windows logo are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners. Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA



1. Gartner, Inc., "CIO Survey Shows the Continuing Importance of Mobile Applications" by Nick Jones, October 30, 2006 [↑](#footnote-ref-2)
2. U.S.: The Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Sarbanes-Oxley Act (SOX); Canada: the Personal Information Protection and Electronic Documents Act (PIPEDA), Personal Health Information Protection Act (PHIPA); United Kingdom: Data Protection Act (DPA); Asia Pacific: Asia-Pacific Economic Cooperation Telecommunications Working Group (APECTEL) [↑](#footnote-ref-3)
3. Windows XP Professional, Windows Vista Business, Windows Vista Enterprise, or Windows Vista Ultimate. [↑](#footnote-ref-4)