

# Contents at a Glance

<b><i>Introduction .....</i></b>	<b><i>1</i></b>
<b><i>Part I: Vista Security Essentials.....</i></b>	<b><i>7</i></b>
Chapter 1: Getting Up to Speed on Vista Security.....	9
Chapter 2: Setting Up Your Security Plan.....	25
Chapter 3: Dispensing Security from Windows Security Center .....	41
<b><i>Part II: Controlling Access to Systems and Data.....</i></b>	<b><i>51</i></b>
Chapter 4: Administering User Account Control.....	53
Chapter 5: Protecting Your Data with Rights Management Service.....	73
Chapter 6: Managing Accounts, Groups, and Shares.....	81
Chapter 7: Advanced Techniques for Managing Access .....	103
<b><i>Part III: Preserving and Protecting Data.....</i></b>	<b><i>133</i></b>
Chapter 8: Backing Up So You Can Always Restore.....	135
Chapter 9: Planning and Implementing Encrypting File System .....	159
Chapter 10: Avoiding Data Theft with BitLocker.....	171
<b><i>Part IV: Guarding against Threats to Network Security ...</i></b>	<b><i>197</i></b>
Chapter 11: Configuring Your Firewall.....	199
Chapter 12: Locking Down Wireless.....	217
Chapter 13: Implementing IE7 Security Features to Limit Your Exposure .....	237
Chapter 14: Avoiding Invasion (By Malware, Spyware, Viruses, and the Other Usual Suspects) .....	259
<b><i>Part V: Establishing Advanced Security Practices .....</i></b>	<b><i>281</i></b>
Chapter 15: Restricting the Use of Removable Media (And More).....	283
Chapter 16: Working with Vista Security Policies .....	293
<b><i>Part VI: The Part of Tens .....</i></b>	<b><i>311</i></b>
Chapter 17: Nine Security Risks and How to Thwart Them.....	313
Chapter 18: Ten Additional Security Tools and Resources You Shouldn't Compute Without .....	325

***Appendix A: Glossary of Vista and Security Terms .....335***  
***Appendix B: Getting to Know Vista Versions  
(And Related Security Features).....341***  
***Index .....345***

<http://www.pbookshop.com>

# Table of Contents

---

<b><i>Introduction</i></b> .....	<b>1</b>
About This Book.....	1
Conventions Used in This Book .....	1
What You're Not to Read.....	2
Foolish Assumptions .....	2
How This Book Is Organized.....	2
Part I: Vista Security Essentials .....	3
Part II: Controlling Access to Systems and Data .....	3
Part III: Preserving and Protecting Data .....	3
Part IV: Guarding against Threats to Network Security .....	4
Part V: Establishing Advanced Security Practices .....	4
Part VI: The Part of Tens .....	4
Icons Used in This Book.....	5
Where to Go from Here.....	5
<b><i>Part 1: Vista Security Essentials</i></b> .....	<b>7</b>
<b>Chapter 1: Getting Up to Speed on Vista Security</b> .....	<b>9</b>
Seeing What's New in Vista Security.....	9
The Vista User Account Control.....	10
Windows Defender .....	11
Parental Controls.....	12
Wireless security enhancements.....	13
Service hardening.....	14
Internet Explorer 7 .....	15
Encryption with EFS and BitLocker .....	16
Windows Security Center enhancements .....	17
Windows Firewall enhancements .....	18
Knowing What to Secure .....	19
Hardware and software.....	19
Personally Identifiable Information (PII) .....	20
Sensitive information from work.....	21
Other information that can be used adversely .....	22

Filling Up Your Security Toolbox.....	22
Understanding your requirements.....	22
Arming yourself with technical tools.....	23
Integrating Common Sense and Security .....	24
<b>Chapter 2: Setting Up Your Security Plan .....</b>	<b>25</b>
Understanding the Risk.....	26
Assessing Your Systems' Security Risks .....	26
Understand your system.....	27
Identify threats .....	27
Identify system vulnerability.....	27
Identify what you have in place (Or can put in place) .....	28
Assess the chance of a security breach .....	28
Know the true effect.....	28
Determine the risk.....	28
Taking action to reduce risk.....	29
Understanding Your System .....	29
Hardware and software.....	30
Interfaces .....	31
System usage and what type of information is on it.....	31
Identifying Threats.....	31
Vulnerability Identification .....	33
What Safeguards Do You Currently Have in Place? .....	34
Telling the Future: What Are the Chances of That Happening? .....	35
Understanding the Real Impact.....	36
Determining the Risk .....	37
Establishing Your Security Plan .....	38
Taking action to reduce the risks .....	38
A little about how users introduce security risks.....	39
<b>Chapter 3: Dispensing Security from Windows Security Center ...</b>	<b>41</b>
Windows Security Center Essentials .....	41
Managing Firewall Settings .....	43
Monitoring, alerting, and remediation.....	43
Using WSC Options menu to manage Firewall.....	43
Configuring Automatic Updating.....	44
Monitoring, alerting, and remediation.....	45
Managing Automatic Updating .....	45
WSC Malware Protection.....	46
Monitoring, alerting, and remediation.....	46
Virus Protection options .....	47
Windows Defender options .....	47
Accessing Other Security Options with WSC .....	47
Internet Security Settings .....	47
User Account Control .....	49
Other things to know .....	49

## ***Part II: Controlling Access to Systems and Data .....51***

### **Chapter 4: Administering User Account Control .....53**

Understanding Life As a Standard User .....	54
Knowing what you can't do.....	55
Admin Approval mode: When Standard User mode isn't enough .....	55
Over-the-Shoulder Credentials .....	57
Evaluating a user's need for access .....	58
Managing UAC with Local Security Policy Settings .....	59
Admin Approval Mode for Built-in Administrators.....	59
Behavior of the Elevation Prompt for Administrators in Admin Approval Mode.....	61
Behavior of the Elevation Prompt for Standard Users .....	63
Detect Application Installations and Prompt for Elevation .....	65
Only Elevate Executables That Are signed and Validated.....	66
Only Elevate UIAccess Applications That Are Installed in Secure Locations.....	67
Run All Administrators in Admin Approval Mode .....	69
Switch to the Secure Desktop When Prompting for Elevation .....	70
Virtualize File and Registry Write Failures to Per-User Locations.....	71

### **Chapter 5: Protecting Your Data with Rights Management Service .....73**

What Is RMS? .....	73
Why you might need to use RMS.....	74
How RMS client integrates your machine .....	74
RMS management features.....	75
Microsoft Office Information Rights Management (IRM) Capabilities .....	76
IRM and Outlook.....	76
IRM and documents .....	78
Rights Management add-on for Internet Explorer.....	79
Digital Rights Management (DRM) versus RMS .....	80
Drawbacks to RMS .....	80

### **Chapter 6: Managing Accounts, Groups, and Shares .....81**

The Vista Identity Model.....	81
Managing Accounts and Groups within Vista.....	82
Vista Built-in Accounts and Groups.....	83
Administrator.....	83
Administrators.....	84
ANONYMOUS LOGON.....	84
Backup Operators .....	84
BATCH.....	84
Event Log Readers.....	85
Everyone.....	85
Guest .....	85

IIS_IUSRS .....	85
INTERACTIVE .....	85
IUSR .....	86
LOCAL SERVICE .....	86
NETWORK .....	86
Network Configuration Operators .....	86
NETWORK SERVICE .....	86
Performance Log Users .....	87
Performance Monitor Users .....	87
SERVICE .....	87
SYSTEM .....	87
Users .....	87
Creating and Disabling User Accounts .....	88
Creating a user account and password .....	88
Disabling/re-enabling a user account .....	90
Using the Select Objects Interface .....	90
Creating Groups and Assigning Users .....	94
The Vista Access Control Model .....	96
System security settings .....	96
Object-level security .....	96
Allowing Access to Data through Sharing .....	97
File sharing .....	98
Using a wizard to manage file sharing .....	98
Public folder sharing .....	101
Password-protected sharing .....	101
File or printer sharing and firewalls .....	101

## **Chapter 7: Advanced Techniques for Managing Access . . . . . 103**

Managing Object-Level Security .....	103
Effective permissions .....	105
Inherited versus explicit security .....	108
Protecting the File System through NTFS Permissions .....	111
Understanding How to Lock Down the Registry .....	116
Using Regedit to view and modify the registry .....	118
Registry keys to pay attention to .....	123
Keeping an Eye on Your System .....	124
Auditing and logging policies .....	125
Defining object auditing .....	130

## **Part III: Preserving and Protecting Data . . . . . 133**

### **Chapter 8: Backing Up So You Can Always Restore . . . . . 135**

Why Should I Back Up My Data? .....	136
Choosing Your Vista Backup Options .....	137
Vista system restore point .....	137
Backing up files and folders .....	138
CompletePC Backup .....	139

Shadow Copy .....	139
Supported devices .....	140
Identifying Your Requirements.....	140
Putting Your Requirements to Paper.....	143
Planning Your Backup and Recovery Strategy.....	145
Preserving Your System .....	147
Creating a restore point.....	147
Restoring your system to a previous system state.....	149
Organizing Your Data So It's Easy to Back Up .....	150
Backing Up with Backup and Restore .....	151
Backing up files with the Backup Files Wizard .....	152
Restoring files and folders .....	153
Backing Up with CompletePC Backup.....	154
Restoring a CompletePC Backup.....	155
A little about shadow copying.....	156
<b>Chapter 9: Planning and Implementing Encrypting File System . . .</b>	<b>159</b>
Encryption 101 .....	159
Symmetric encryption .....	160
Asymmetric encryption.....	160
Protecting Your Files and Folders with EFS.....	161
How Encrypting File System works.....	163
Encrypting folders.....	164
Encrypting a specific file.....	166
Sharing encrypted files.....	166
Data recovery.....	167
Developing a file and folder encryption strategy.....	168
<b>Chapter 10: Avoiding Data Theft with BitLocker . . . . .</b>	<b>171</b>
Keeping Data Safe with BitLocker .....	172
BitLocker Requirements.....	173
Preparing Your System for BitLocker .....	174
Preparing a disk with no installed OS.....	174
Preparing a disk with an operating system installed on it.....	176
Setting Up BitLocker .....	178
Enabling BitLocker with basic options.....	179
Enabling BitLocker with advanced options .....	181
Enabling BitLocker on a system without a TPM chip.....	182
Adding additional authentication with TPM plus a PIN or a TPM startup key .....	183
Configuring Additional Security .....	187
Encryption methods .....	188
Prevent memory overwrite.....	189
Recovering BitLocker-protected data.....	191
Recovery folder options .....	191
Configuring recovery options.....	192
Performing a recovery .....	194
Turning Off BitLocker .....	195
Knowing What BitLocker Can't Protect.....	196

**Part IV: Guarding against Threats to Network Security... 197**

<b>Chapter 11: Configuring Your Firewall</b> .....	<b>199</b>
Using the Windows Firewall Applet .....	199
General tab .....	201
Exceptions tab .....	202
Advanced tab .....	204
Using Windows Firewall with Advanced Security Applet .....	205
Using the Getting Started Section to configure Firewall.....	211
Using the Resources pane .....	213
What Do I Do Now? .....	214
Other Firewalls .....	215
<b>Chapter 12: Locking Down Wireless</b> .....	<b>217</b>
Wireless Network Basic Training .....	218
What's New for Wireless Security in Vista .....	220
Configuring Wireless Security in Vista .....	221
Connecting to a network .....	221
A few words about unsecure networks .....	222
Accessing wireless hotspots or other unsecure wireless networks .....	223
Restricting use to specific wireless networks .....	224
Network and Sharing Center .....	225
Modifying your network connection.....	226
Configuring static IP addresses .....	228
Setting up an ad hoc (peer-to-peer) wireless network .....	230
Securing Your Wireless Router or Access Point.....	232
Change your administrative username and password.....	232
Change your service set identifier (SSID) .....	233
Enabling secure communication .....	233
Consider disabling DHCP .....	234
MAC address filtering .....	235
Disabling SSID broadcasts.....	235
Know your network's range and limit it if needed .....	236
<b>Chapter 13: Implementing IE7 Security Features to Limit Your Exposure</b> .....	<b>237</b>
Configuring IE7 Internet Protected Mode Options .....	237
Working Safely with ActiveX.....	241
Protecting against Cross-Domain Scripting Attacks .....	243
Configuring Phishing Filters .....	244
Setting Binary Behavior Restrictions .....	246
Understanding Local Machine Zone Restrictions.....	247
Adding more security with MIME safety and MK protocol restriction settings .....	249
Locking down network protocols to prevent exposures .....	250

Controlling object caching .....	253
Controlling automatic downloads and scripts .....	256
Bringing It All Together .....	257
<b>Chapter 14: Avoiding Invasion (By Malware, Spyware, Viruses, and the Other Usual Suspects) .....</b>	<b>259</b>
The 411 on Unsanctioned Software .....	259
Reducing Spyware, Malware, and More with Windows Defender .....	261
What's New .....	261
Defending Your System .....	262
Getting to know the Windows Defender interface .....	262
Updating Windows Defender definition files .....	262
Real-time protection.....	263
Invoking on-demand scans.....	266
Responding to threats .....	269
Putting Defender's tools to work.....	272
Lending a helping hand in classifying spyware .....	277
Other ways to protect against spyware, viruses, and other malicious software.....	278
 <b>Part V: Establishing Advanced Security Practices .....</b>	<b>281</b>
 <b>Chapter 15: Restricting the Use of Removable Media (And More) . .</b>	<b>283</b>
Removable Media and Associated Security Risks .....	283
Risks of attaching media .....	284
Risks of detaching media.....	284
Protecting Yourself Against the Risks of Removable Media .....	285
Protecting against viruses and malware .....	285
Protection against removal of data from your machine.....	286
Protection of data on removable devices .....	287
Using Device Control to Protect Data on the Move .....	288
Implementing Device Control installation settings.....	288
Implementing Device Control usage settings .....	289
Controlling device installation.....	290
Controlling device usage .....	292
 <b>Chapter 16: Working with Vista Security Policies .....</b>	<b>293</b>
Implementing the Right Security Settings for You .....	294
Why you should use policy to manage security settings.....	294
Managing policy with the Group Policy Object Editor .....	295
Protecting Your System with Local Security Policy Settings .....	296
Password policies.....	296
Account-lockout policies.....	297
Audit policies .....	298
User rights assignment .....	298

Security options .....	299
Event log .....	300
Diving Deeper into SecurityPolicy Settings .....	300
Computer configuration policy settings.....	301
User-configuration policy settings .....	302
Administrative templates .....	302
Managing Policy by Using Security Templates.....	305
Creating your own custom security template .....	305
Windows Vista Security Guide templates .....	307
Applying a security template to your machine .....	308
<b><i>Part VI: The Part of Tens .....</i></b>	<b><i>311</i></b>
<b>Chapter 17: Nine Security Risks and How to Thwart Them .....</b>	<b>313</b>
Always Being Connected.....	313
Taking Shortcuts with Security .....	314
Failing to Apply Software Patches .....	316
Unwillingly Participating in Attacks .....	317
Getting Careless with E-Mail Security.....	318
Mobile Code.....	319
Peer-to-Peer Networking .....	320
Unsafe Instant Messaging .....	321
Mobile Device Security.....	322
<b>Chapter 18: Ten Additional Security Tools and Resources   You Shouldn't Complete Without .....</b>	<b>325</b>
Antivirus Software.....	325
Spyware Removal Tools .....	326
Third-Party Backup Software.....	327
Firewalls and other Network Protection .....	328
Online Security Newsletters .....	329
The About.com Identity-Theft Web Site .....	330
Microsoft Security Baseline Analyzer.....	330
Vista Security Sidebar Gadgets .....	331
Systinternals Tools.....	332
Secure File-Deletion Software .....	332
<b><i>Appendix A: Glossary of Vista and Security Terms.....</i></b>	<b><i>335</i></b>
<b><i>Appendix B: Getting to Know Vista Versions   (And Related Security Features) .....</i></b>	<b><i>341</i></b>
<b><i>Index.....</i></b>	<b><i>345</i></b>