

# Contents

<b>Chapter 1: Security — The Reasons You’re Reading This Book .....</b>	<b>1</b>
Evaluating Your Risks .....	3
Confidentiality .....	3
Integrity .....	3
Availability .....	4
Privacy .....	5
Evaluating the Threats .....	5
Managing the Strategic Issues .....	6
Control Access to Applications, Data, and Systems .....	6
Review Requirements and Maintain Compliance .....	7
Getting Started .....	8
Don’t Close the Book .....	8
<b>Chapter 2: Policies and Procedures .....</b>	<b>11</b>
Your Security Policy .....	12
Physical Security .....	12
Responsible Parties .....	12
Data Classification .....	13
Network Connections .....	16
Application Design .....	17
Platform-Specific Issues .....	17
Employee Guidelines .....	18
Notification, Enforcement, and Compliance .....	18
Business Events and Procedures .....	19
Getting Started with Your Policy .....	20
Legal Review .....	20
<b>Chapter 3: Security at the System Level .....</b>	<b>21</b>
The System Security Level .....	21
System Value QSECURITY .....	21
Security Level 20 .....	22
Security Level 30 .....	23
Security Level 40 .....	24
Security Level 50 .....	26
Moving to Security Level 40 or 50 .....	28
Security-Related System Values .....	30
General Security System Values .....	30

---

Password-Related System Values .....	48
Audit-Related System Values .....	61
Locking Down Security-Related System Values .....	67
A Helpful Tool .....	67
<b>Chapter 4: The Facts About User Profiles .....</b>	<b>69</b>
What Are User Profiles? .....	69
User Profile Attributes .....	70
USRPRF (User Profile) .....	73
PASSWORD (User Password) .....	75
PWDEXP (Set Password to Expired) .....	76
LCLPWDMGT (Local Password Management) .....	77
PWDEXPITV (Password Expiration Interval) .....	77
PWDCHGBLK (Block Password Change) .....	78
STATUS (Profile Status) .....	78
USRCLS (User Class) and SPCAUT (Special Authority) .....	79
Initial Sign-On Options .....	82
System Value Overrides .....	85
Group Profiles .....	85
UID (User Identification Number) and GID (Group Identification Number) .....	88
USREXPDATE (User Expiration Date) and USREXPITV (User Expiration Interval) .....	88
AUT (Authority) .....	88
Private Authorities and User Profiles .....	89
Helpful Tools .....	89
Navigator for i .....	91
Copying User Profiles .....	92
Validation List Users .....	93
Security Implications of Validation List Users .....	105
<b>Chapter 5: Service Tools Security .....</b>	<b>107</b>
Service Tools User IDs .....	107
Service Tools User ID Passwords .....	109
Service Tools Functional Privileges .....	111
Service Tools Features in V6R1 .....	116
Device Profiles .....	118
The Work with System Security Panel .....	119
Monitoring Service Tools Use .....	120
Service Tools Security Recommendations .....	121

---

<b>Chapter 6: Object-Level Security .....</b>	<b>123</b>
Private Authorities .....	123
Object Authorities .....	124
Data Authorities .....	126
Authority Relationships .....	126
Authority Groupings .....	127
Group Profiles .....	128
Multiple Group Profiles .....	129
Why Grant Authority to Group Profiles? .....	129
Public Authority .....	130
Establishing Public Authority .....	130
Using Default Public Authority .....	132
Authorization Lists .....	134
How IBM i Checks Authority .....	136
Authority Checking Example: Precedence Between Users and Groups .....	138
Authority Cache .....	139
Adopted Authority .....	140
Adopted Authority Example .....	141
Authorities and Save/Restore Functions .....	143
Object Ownership .....	144
Limit User Function .....	146
Helpful Tools .....	149
Navigator for i .....	149
<b>Chapter 7: Security Considerations for the IFS .....</b>	<b>151</b>
IFS Authorities .....	152
Managing Authorities to IFS Objects .....	153
File Attributes .....	154
Adopted Authority and the IFS .....	157
Auditing Objects in the IFS .....	157
File Shares: Accessing Objects in the IFS .....	158
Gotchas and Helpful Hints .....	160
General Cautions .....	160
Creating New Objects .....	160
Copying Objects .....	161
CPYTOSTMF and CPYTOIMPF .....	161
Virus Scanning .....	162
Security Recommendations .....	162
*PUBLIC Authority for Application and User Directories .....	163
*PUBLIC Authority for IBM-Supplied Directories .....	163

Determining Appropriate Authority .....	164
Home Directory .....	164
Web Applications .....	164
QPWFSESERVER Authorization List .....	165
Review (and Remove) File Shares .....	165
Final Advice .....	166
Helpful Tools .....	166
<b>Chapter 8: Securing Your Printed Output .....</b>	<b>167</b>
Security-Related Output Queue Attributes .....	168
DSPDTA (Display Data) .....	168
OPRCTL (Operator Control) .....	169
AUTCHK (Authority Check) .....	169
AUT (Authority) .....	169
*SPLCTL Special Authority .....	170
Output Queue Ownership .....	171
Sample Output Queue Security Implementation .....	171
Helpful Tools .....	173
Navigator for i .....	173
<b>Chapter 9: Encryption .....</b>	<b>175</b>
Encryption Basics .....	175
Public Key Infrastructure .....	176
Transmission of Data .....	177
Encrypting Data in Files .....	178
Identify the Scope of Your Project .....	178
Architecting Your Application to Use Encryption .....	180
The Key Is Key Management .....	181
Encrypting Backup Media .....	183
What IBM Provides .....	184
Encrypted Auxiliary Storage Pools .....	184
Disaster Recovery Considerations .....	184
Success Depends on Planning .....	184
Helpful Resources .....	184
<b>Chapter 10: Connecting to the System .....</b>	<b>185</b>
Physical Security .....	185
System Values .....	186
*IOSYSCFG Special Authority .....	186
Network Security Attributes .....	186

---

JOBACN .....	187
PCSACC .....	187
DDMACC .....	187
Security Considerations for TCP/IP .....	188
Starting TCP/IP Servers .....	188
Securing Ports .....	189
Internal Addresses .....	190
IP Packet Filtering .....	190
NAT .....	190
FTP .....	191
SMTP .....	193
POP .....	193
DNS .....	194
REXEC .....	195
SNMP .....	195
SNTP .....	195
DRDA and DDM .....	196
Security Considerations for PCs .....	198
IBM i Access for Windows .....	198
ODBC Security Considerations .....	200
IBM i Access for Web .....	200
Using Exit Points .....	202
Management Central .....	203
Secure Communications .....	204
Digital Certificates .....	204
Secure Sockets Layer .....	204
Digital Certificate Manager .....	206
Virtual Private Networks .....	206
Secure Shell .....	206
Wireless Considerations .....	207
Helpful Tools .....	208
Navigator for i .....	209
IBM Director .....	209
<b>Chapter 11: Internet Security .....</b>	<b>211</b>
Determine Your Risk .....	211
The Process .....	212
Corporate Security Policy .....	212
Internet Service Provider .....	214
Firewalls .....	214

System Values .....	216
User Profiles .....	217
Resource Security .....	217
Controlling What Goes On .....	218
Secure Web Applications .....	219
Exit Programs .....	221
Monitoring .....	221
Intrusion Detection .....	221
<i>Security Considerations for Outsourcing and the Cloud</i> .....	222
Security Configuration .....	225
Testing and Evaluation .....	225
Business Contingency Plan .....	225
Be Careful Out There .....	226

## **Chapter 12: Evaluating Applications' Current Implementations**

<b>and Designing New Ones</b> .....	<b>227</b>
From the Beginning .....	228
Design Considerations .....	228
What Roles Will Use the Application? .....	229
Common Authorization Schemes .....	230
Application Ownership .....	235
Which Profile Runs the Application and Is There Adequate Logging? .....	235
Does the Application Require a "Powerful" Profile? .....	235
What Kind of Audit Trail Does the Application Require? .....	236
Implementation Details .....	237
Set IBM i Authorities .....	237
Define *PUBLIC Authority .....	237
<i>Security Questionnaire for Vendors</i> .....	238
Secure Job Descriptions .....	239
Manage Your Library List .....	239
Make Library-Qualified Calls .....	239
Don't Store Passwords in Clear Text .....	240
Testing, Testing .....	240
Moving Forward .....	241

## **Chapter 13: Role-Based Access** ..... **243**

Roles .....	243
Defining the Roles .....	244
Group Profiles .....	245
Why Group Profiles? .....	246
Implementation .....	247

<b>Chapter 14: Role-Based Access for IT .....</b>	<b>249</b>
Security and Your IT Staff .....	249
Identify the Roles .....	250
Define a Secure Environment for Each Business Function .....	251
Operator .....	251
Network Administrator for IBM i .....	253
Help Desk .....	253
Programmer/Analyst .....	254
System and Security Administrators .....	256
Security for Vendors and Consultants .....	257
Vendor Support .....	258
Consultant Practices .....	258
Role-Based IT Access .....	259
<b>Chapter 15: Auditing .....</b>	<b>261</b>
The History Log .....	262
History Log Housekeeping .....	264
Inside Information .....	264
The Security Audit Journal .....	264
The Audit Journal .....	265
Auditing Controls .....	266
System-Wide Auditing .....	266
Other Auditing Values .....	269
User Auditing .....	270
Object Auditing .....	271
Object Auditing for New Objects .....	274
Event-Auditing Recommendations .....	274
Auditing Controls Security Recommendations .....	275
System and User Event-Auditing Security Recommendations .....	275
Object-Auditing Recommendations .....	275
Working with the Audit Journal .....	275
Understanding Journal Entry Formats .....	276
Displaying and Printing Audit Journal Entries .....	278
Using the DSPAUDJRNE Command to Display Entries .....	279
Using the DSPJRN Command to Display Entries .....	279
Using the CPYAUDJRNE Command .....	281
Reporting on Activities from the Information in the Audit Journal .....	284
Benefits of the IBM i Architecture .....	286
Helpful Tools .....	286
Navigator for i .....	287

<b>Chapter 16: Implementing Object-Level Security .....</b>	<b>289</b>
Determine the Scope of Your Project .....	289
High-Level Design of the Architecture .....	291
Building the Big Picture .....	291
Collecting the Information .....	293
Dynamic SQL .....	295
Decision Points .....	296
Owning All Application Objects Rather Than Being Authorized .....	296
What Adopts .....	297
Authorization Lists .....	298
*PUBLIC Authority .....	298
Queries .....	300
Making Changes to the Application .....	301
Rolling Out the Changes .....	303
Changes to Change Management .....	304
When Something Breaks: Debugging and Recovery Techniques .....	304
Making Sure the Changes “Stick” .....	305
Gotchas .....	305
Summary .....	306
<b>Chapter 17: Security Administration .....</b>	<b>307</b>
Remove Obsolete Objects .....	307
System Values .....	308
User Profiles .....	308
Managing Authorities .....	310
Regular Reviews .....	310
Controlling Who Can Do What .....	311
Integrated File System (IFS) .....	311
Regular Updates .....	312
Summary .....	312
<b>Chapter 18: Maintaining Compliance .....</b>	<b>313</b>
Evaluating the Key Areas .....	314
System Values .....	314
User Profiles .....	315
Object Authority .....	316
An Annual Security Assessment .....	317
Regular Reviews .....	318
Group Profile Membership and Special Authority Assignments .....	319
Authorization Lists .....	319



Policies and Processes .....	320
Summary .....	321
<b>Chapter 19: Preparing for the Worst: Creating a Security Incident</b>	
<b>Response Plan .....</b>	<b>323</b>
Be Prepared .....	323
Assembling the Incident Response Team .....	324
Responding to an Incident .....	325
Data Preservation .....	325
Performing the Investigation .....	326
Be Proactive .....	326
Make Sure You're Saving the Right Information .....	326
Saving Security Data .....	326
Restoring Security Data .....	327
Re-Creating the System After a Breach .....	329
<b>Chapter 20: Creating a Security Awareness Program .....</b>	<b>331</b>
What Method Do I Use to Communicate? .....	332
Getting Started .....	333
<b>Index.....</b>	<b>335</b>