Contents

I PRINCIPLES 1

1. Historical Roots 3
   The Industrial Revolution 3
   Scientific Management 4
   Human Relations 4
   Operations Research 5
   Age of Technology 6
   Business Today 7

2. Strategy 11
   Core and Support Activities 12
   Outsourcing 12
   Risks 14
   The Importance of Technical Knowledge 15
   Predict, Quantify, and Control 16
   Strategy Imperatives 16
   Strategic Planning 18
   Effect of Policy on Planning 20

3. Leading 23
   Focus on the Future 23
   Manager versus Leader 24
   Competencies 24
   Empowerment 25
   Conflicting Values 26
   Following 26
   Adding Value 27
   Competition 27
   Loyalty 28
   Price of Leadership 28
   Leading in the 21st Century 29

4. Organizing the Security Group 33
   Staffing 33
   The Independent Contractor 38
   The Practices of Organizing 39

Setting Objectives 39
Resourcing to Meet Targets 41
When Security Is a Line Responsibility 43
Assigning Tasks 44
Monitoring 45
Terminating an Employee 45
Managing the Interview 47
Organizational Structures 47
The Security Group Fit 51

5. Managing People 53
Maslow's Theory 53
Maslow in the Security Environment 55
People Development 56
Performance Appraisal 58
Setting Targets 59
Reviewing Performance 60
The Performance Appraisal Cycle 62
Merit Rating 64
Upward Feedback 66
Position Evaluation 69

6. Managing Resources 73
Budgeting 73
The Zero-Based Budget 74
Controlling Costs 79

7. Managing Change 85
Designing Change 86
Working Through People 86
Teamwork in Effecting Change 87
Familiar but Not Understood 88
Technology and Change 89
The Politics of Change 89
Dealing with Change on a Personal Level 91
Action Coaching 92

8. Decision Making 95
Frame the Issue 95
Collect Information 96
Decide 96
Examine Feedback 97

II ADMINISTRATION 99

9. Risk Management 101
Assets Identification 101
Threat Identification 102
Probability Assessment 102
Impact Assessment 102
Frequency Assessment 104
Manageability Assessment 104
Identification of Countermeasures 105
Review and Audit Technique 108
Reporting the Results 117
Follow-up 118
Project Review Technique 118
Security Incident Causation Model (SICM) 120
Applying the SICM Technique 124
Summary 124

10. Security Officer Operations 125
Background 125
Developing the Protective Scheme 125
Staffing 126
Skills Needed 127
Tools and Equipment 127
Proprietary versus Contract Security 128
Selecting a Contractor 128
Contract Performance 132
Security Officer Supervision 133
Monitoring 134
Determining the Value of Security Officer Services 134
Understanding the Contractor 135
Mutual Respect 135
Legal Issues 136
Guard Dogs 138
Life Safety 140

11. Physical Security 143
Background 143
Facility Protection 143
Choosing the Safeguards 144
Starting at the Perimeter 144

Protective Barriers 145
Protective Lighting 147
Intrusion Detection 148
Monitoring and Communication 150
Tamper Detection 151
Sensor Types 151
Lock and Key Systems 153
Types of Locks 153
Key Control 155
Conclusion 160

12. Access Control 161
Introduction 161
Employee Badges and Visitor Passes 161
Types of Identification Cards 162
Traffic Control 164
Materials Control 165
Physical Security 167
Layered Protection 168
Business Rationale 168
Closed-Circuit Television (CCTV) 169
Intrusion Detection 173
Threat Analysis 175

13. Investigations 179
Internal Theft 179
Fraud 181
Characteristics of Fraud 183
Bribery 183
Frauds Committed by Outsiders 184
Workers' Compensation Fraud 189
Problems in Prosecuting 191
The Forensic Investigator 191
Compliance Investigations 191
Whistle-Blower Rules 192
Investigative Intelligence Gathering 192
Interview and Interrogation 193
Kinesics 210
Polygraph 213
Physical Evidence 215
Forensic Tests 216
Incident Scene 225
Security Officer Involvement 225
Investigative Photography 226
Testifying 229

14. Preemployment Screening 235
Records Checking 235
References Checking 236
Drug and Alcohol Testing 238
Paper and Pencil Testing 239
Validity 240
Problems in Design and Interpretation 240
The Fair Credit Reporting Act 241

15. Emergency Management 243
Anticipation 243
Preparation 244
Prevention and Response 245
Business Continuity 246
Fire Emergencies 247
Medical Emergencies 254
Natural Disasters 261
Severe Windstorm 263
Standard Operating Procedures 265
Dealing with the Media 267

16. Management of Bomb Incidents 271
Planning 272
The Bomb Threat 277
Bomb Types 282
The Aftermath 285

17. Information Security 287
Introduction 287
Sensitive Information 289
Proprietary Information 291
Data Protection 293
Data and Dollars 293
Risk Assessment of Information Systems 297
Cybervandalism 301
Employee Behaviors 303
The Intranet 303
Protective Techniques 304
Industrial Espionage 306
Competitive Intelligence 312
Product and Process 313

18. Substance Abuse Prevention 317
The Rationale for Prevention 317
The Security Leader's Role in Prevention 318
Testing for Illegal Drugs 319

Testing for Alcohol 322
Working Through Others 323
The Indicators of Abuse 331
Substance Abuse Investigations 333

19. Executive Protection 335
Kidnap Prevention 335
Kidnap Planning 336
Abduction 340
The Personal Security Mission 342
Event-Based Protection 346
Absolute Protection Is Not Possible 349

20. Workplace Violence 351
Forming a Team 351
Assessing Readiness 352
Conducting an Assessment Audit 354
Developing Plans and Procedures 355
Workplace Violence Policy 360
The Warning Signs 361
Stalking 363
Psychological Profiling 366
Training 367
Preventive Techniques 369
Nondisclosure of Potential Violence 370
Implications of the Americans with Disabilities Act 371

21. Security Awareness 373
Three Dimensions 373
Awareness Is an Ongoing Process 374
Awareness Is Local 374
Modes for Promoting Awareness 374
Avoiding Apathy 374
Choosing, Formulating, and Presenting the Message 375
The Spotlight 376

Endnotes 377

Index 383