

Table of Contents

Introduction	XIII
Acknowledgements.	XIV
Chapter 1: Data Protection Regulations	1
The Basis of Data Protection	1
Privacy	1
Intellectual Property.	2
National Security	2
Data Protection Regulations Addressing Personal Information	3
Early Recognition of Data Protection’s Role in Regulations	3
Federal Regulations including Data Protection Requirements (1990-2000)	4
<i>The Health Insurance Portability and Accountability Act</i>	4
<i>The Financial Services Modernization Act of 1999</i>	8
<i>The Impact of Identity Fraud on Data Protection Legislation</i>	9
<i>The Fair and Accurate Credit Transactions Act</i>	10
<i>The Public Company Accounting Reform and Investor Protection Act</i>	12
<i>State Data Protection Laws</i>	13
Consistent Elements of Data Protection Regulations	14
<i>The Reasonableness Standard</i>	14
<i>Designation of Accountability</i>	15
<i>Written Procedures and Employee Training</i>	16
<i>Vendor Selection Due Diligence</i>	17
Information Disposition and the U.S. Supreme Court	18
Information Disposition Requirements of Legacy Custodians.	19
<i>Indiana</i>	19
<i>California</i>	19
Data Protection Regulations Addressing Intellectual Property Rights	20
The Economic Espionage Act (EEA) of 1996	20
Data Protection Regulations Addressing National Security Information	21
Conclusion	22
Appendices	23
Appendix A: Data Destruction Requirements at the State Level	23
Appendix B: State-Level Data Breach Notification Regulations	24
Appendix C: HIPAA Regulatory Chart	26

Information Disposition

Appendix D: GLBA Regulatory Chart	28
Appendix E: FACTA Regulatory Chart	29
Appendix F: Sample/Proposed Information Destruction Regulation	30
Sources	35
Chapter 2: Physical Security	37
Staging of Materials Prior to Disposition	37
Staging of Controlled Records	37
Staging of Incidental Records	38
Collection Containers	38
Centralized Collection Containers	39
<i>Collection Container Capacity Restrictions</i>	39
<i>Collection Container Security</i>	40
<i>Deskside Collection Containers</i>	40
<i>Key Control</i>	41
<i>Custody</i>	42
Boxes and Pallets	43
Electronic Media Collection and Staging	43
<i>Assigning a Unique Identifier</i>	44
<i>Tagging IT Assets</i>	44
<i>Sealing IT Assets</i>	45
In-House Information Destruction Strategies	45
Decentralized In-House Destruction	46
Centralized In-House Destruction	47
Special Collection Issues	48
Allowing Employee Discretion	48
Workstation Collection	48
Need-to-Know and Principle of Least Privilege	48
Preservation Orders	49
Clean Desk Policy	49
Reconciliation of Disposed Electronic Assets	50
Physical Security for Information Disposal Services	51
Physical Security in the Field	51
<i>Collecting Incidental Media and Information</i>	52
<i>Collecting Consolidated Media</i>	53
<i>On-site Destruction Security</i>	53
<i>Transporting Media</i>	54
<i>Physical Security of Destruction Facilities</i>	55
<i>Access Control and Key Systems</i>	55

<i>Credentialing and Signage</i>	56
<i>Video Surveillance and Alarm Monitoring</i>	57
Conclusion	58
Sources	58
Chapter 3: Records and Information Management (RIM) Principles	59
Records Creation	59
Classification of Records	60
Disposition of Controlled Records	61
Liability of Retaining Unnecessary Records	62
<i>Legal Discovery</i>	62
<i>The Risk of Adverse Inference</i>	62
<i>Increasing Risk of Unauthorized Access</i>	63
<i>Retained Records on Non-Paper Media</i>	63
Disposition of Duplicate Records	63
Disposition of Incidental Records	64
The Certificate of Destruction	65
What Was Destroyed	65
Who Destroyed It	66
Time and Location of Destruction	67
Basic Certificate of Destruction Itemization Strategies	68
How it was Destroyed	68
Information Destruction and the Cloud	68
Audit Trail and Transactional Record	68
What a Certificate of Destruction is Not	69
Discrepancies	70
Authorization Prior to Disposition	71
The Information/Asset Destruction Authorization Form	73
Authorizing Agents	74
Data and Information Migration	76
Conclusion	76
Appendix	77
Appendix A: Case Law Related to Sporadic or Undisciplined Records Disposition	77
Sources	78
Chapter 4: Risk Management Principles	79
Personnel	79
Screening	80
Procedures and Training	81

Information Disposition

Acknowledgements and Agreements.	81
Access Restrictions.	81
Demonstrability	82
Indemnification.	82
Coverage Orientation	84
<i>Breach Mitigation Teams</i>	84
<i>Breach Notification Coverage</i>	85
Contracts	85
Liability Transfer and Indemnification Provisions	86
Regulatory Linkage Provisions.	87
<i>Breach Notification</i>	87
<i>Operational Security Specifications.</i>	88
<i>Employee Training/Written Procedures.</i>	88
<i>HIPAA Business Associate Agreement</i>	88
<i>The Financial Services Modernization Act Safeguards Rule</i>	89
<i>Other Data Protection Regulations.</i>	89
Exclusivity Provisions	89
Transfer or Acceptance of Custody	90
Subcontractor Provisions	91
Negotiable Instruments	91
Transferability Provision.	92
Service Provider Selection.	92
Service Provider Certifications.	93
Conclusion	95
Sources	95
Chapter 5: Information Protection Principles	97
Copyright Protection	98
Registration of Trademarks	99
Trade Secret and Intellectual Property Protections	100
Information Classification.	100
Access Control	101
National Security Information (NSI)	102
General Information Protection Controls.	102
Authentication	103
Data Encryption	103
Challenges to Encryption as a Data Protection Control	104
<i>User Accountability</i>	105
<i>“Key” Protection.</i>	105

<i>Overconfidence</i>	105
<i>Catastrophic Loss</i>	105
<i>Brute Force Attacks</i>	106
Hash Function Encryption	106
Encryption and Information Disposition	106
Protecting Information While Traveling	107
Protecting Electronic Media and Information While Traveling	107
Protecting Hard-Copy Media and Information While Traveling.	108
Employee Discretion	108
Conclusion	109
Appendices	110
Appendix A: Copyrights and Trademarks	110
Appendix B: National Security (Classified) Information (NSI)	112
Sources	113
Chapter 6: Secure Destruction Methodologies	115
On-Site and Off-Site Service Platforms	115
Equipment and Software Certifications	116
Electronic Media Erasure	116
Overwriting Magnetic Media	116
Limitations to the Hard Drive Overwriting	117
<i>Defective Sectors</i>	118
<i>Hybrid Hard Drives</i>	118
Overwriting Solid-State Memory Devices	118
Overwriting Magnetic Tape	119
Equipment Connectivity and Overwriting	119
Degaussing Magnetic Media.	121
Limitations of Degaussing.	121
Cryptographic Erasure.	122
Quality Control for Electronic Erasure Processes	122
Physical Destruction Methods and Systems	125
Pulping/Pulper	125
Dissolution	126
Disintegration/Disintegrators	127
Pulverization/Hammermill	128
Grinding/Grinders	129
Shredding/Shredders	129
<i>Continuous Strip Shredders</i>	130
<i>Cross-Cut Shredders</i>	131
<i>Pierce and Tear Shredders</i>	131

Information Disposition

Shredders Focused on Small Electronic Devices	131
Disabling	132
Process/Particle Size Standards, Guidance and Requirements	132
NIST 800-88: Guidelines for Media Sanitization	133
Internal Revenue Service (IRS) Publication 1075	134
Payment Card Industry (PCI) Data Security Standards	134
Irrelevant Standards	136
Sources	137
Chapter 7: Information Disposition Policies and Procedures	139
Why Start With Information Disposition Policies And Procedures	140
Policies Are Not Procedures.	140
The Information Disposition “Policy”	141
1.0 Organizational Accountability	141
1.1 Acceptance of Responsibility	141
1.2 Assignment of a Compliance Officer	141
1.3 Policy Development, Implementation and Oversight	141
1.4 Employee Training	141
1.5 Information Destruction Policy Directory	142
2.0 Information Destruction Processes	142
3.0 Qualifications/Selection of Approved Service Provider(s)	142
4.0 Compliance	142
4.1 Auditing Compliance	142
4.2 Information Preservation	142
5.0 Information Transferred to Third Parties	143
The Information Disposition “Procedures”	143
Media-Specific Destruction Procedures	144
Procedural Elements Not Specific to Media Type	146
Employee Training Procedures	146
Information Destruction Policy Directory	146
Vendor Selection Procedures	147
Auditing Procedures.	147
Preservation of Records	148
Virtual Subcontractor Networks	148
Evaluating/Specifying Service Provider Certifications	148
Evaluating/Specifying Service Provider Indemnification	149
Emerging Information Disposition Procedural Issues	150

Appendices	152
Appendix A: (Detailed) Information Disposition Procedural Options	152
1.0 Introduction and Overview	152
1.1 Destruction of Information-bearing Media	152
1.2 Policy Development, Implementation and Oversight	152
1.2.1 Assignment of Compliance Officer	152
1.2.2 Policy Development	153
1.2.3 Procedure Development and Review:	153
1.2.4 Policy and Procedures Approval	153
1.2.5 Orientation & Training	153
1.2.6 Contracting/Purchasing	153
1.2.7 Compliance Auditing/Review	154
1.2.8 Posting/Filing	154
1.3 Employee Orientation/Training	154
1.3.1 Orientation/Training	154
1.3.2 Acknowledgement	155
1.4 Information Destruction Policy Directory	155
2.0 Information Destruction Procedures	156
2.1 Paper Media	156
2.1.1 Authorization for Destruction of Paper Media	156
2.1.1.1 Paper Media (Retained/Controlled)	156
2.1.1.2 Paper Media (Incidental Records)	156
2.1.2a Securing Paper Media Prior to Destruction (Retained/Controlled Records)	157
2.1.2b Securing Paper Media Prior to Destruction (Incidental/Duplicate Records)	157
2.1.3 Approved Methods for Destruction of Paper Media	158
2.1.4 Disposal of Destroyed Paper Media	160
2.1.5 The Audit Trail for Destruction of Paper Media	160
2.1.5.1 Retained/Controlled Paper Media	160
2.1.5.2 Incidental Paper Records [no authorization is required]	161
2.2 Micro Media	161
2.2.1 Authorization for Destruction of Micro Media	162
2.2.2 Securing Micro Media Prior to Destruction	162
2.2.3 Methods for Destruction of Micro Media	162
2.2.4 Disposal of Destroyed Micro Media	164
2.2.5 The Audit Trail for Destruction of Micro Media	165
2.3 Optical Media (CD/DVD)	165
2.3.1 Authorization for Destruction of Optical Media	166
2.3.2 Securing Optical Media Prior to Destruction	166

Information Disposition

2.3.3 Methods for Destruction of Optical Media	166
2.3.4 Disposal Method of Destroyed Optical Media	168
2.3.5 The Audit Trail for Destruction of Optical Media	169
2.4 Electronic Equipment with Magnetic Storage Media (EMag)	169
2.4.1 Authorization for Destruction of EMag.	169
2.4.2 Segregating and Securing EMag Prior to Destruction	170
2.4.2.1 EMag from Centralized/Core Operating Units.	170
2.4.2.2 EMag from Remote/Satellite Operating Units (if applicable)	170
2.4.3 Methods for Destruction of EMag	171
2.4.4 Disposal Methods of Destroyed/Degaussed EMag	175
2.4.4.1 Mechanically Destroyed or Degaussed EMag.	175
2.4.4.2 Overwritten EMag	175
2.4.5 Quality Control for EMag Erasure Processes	175
2.4.6 The Audit Trail for EMag Destruction	177
2.5 Solid State Memory Devices	178
2.5.1 Authorization for Destruction of Solid State Memory Devices	178
2.5.2 Segregating and Securing Solid State Memory Devices Prior to Destruction	178
2.5.3 Methods for Destruction of Solid State Memory Devices	179
2.5.4 Disposing of Destroyed Solid State Memory Devices	180
2.5.5 The Audit Trail for Destruction of Solid State Memory Devices	180
2.6 Information-bearing Equipment (Owned by the Data Controller)	181
2.7 Information Bearing Equipment (Leased)	181
2.8 Cash-Value Instruments	182
2.8.1 Authorization for Destruction of Cash-Value Instruments	182
2.8.2 Segregating and Securing Cash-Value Instruments Prior to Destruction	182
2.8.3 Methods for Destruction of Cash-Value Instruments	182
2.8.4 Disposal Methods of Destroyed Cash-Value Instruments	184
2.8.5 The Audit Trail for Destruction of Cash-Value Instruments	184
2.9 Prototypes/Product Samples/Off-Specification Products	185
2.9.1 Authorization for Destruction of Prototypes/Product Samples/Off Spec. Products	185
2.9.2 Segregating and Securing Prototypes/Product Samples/Off Spec. Products Prior to Destruction	185
2.9.3 Methods for Destruction of Prototypes/Product Samples/Off Spec. Products	186
2.9.4 Disposal Methods of Destroyed Prototypes/Product Samples/Off-Specification Products	187
2.9.5 The Audit Trail for Destruction of Prototypes/Product Samples/Off-Specification Products.	187
2.10 Disposition of Information Remotely Stored on Non-Proprietary Platforms	188
3.0 Qualifications and Selection of an Approved Service Provider	188
4.0 Policy Compliance	190
4.1 Auditing Service Provider Compliance	190

<i>4.2 Auditing Internal Compliance</i>	191
<i>4.3 Litigation Hold/Preservation Order</i>	191
<i>5.0 Information Transferred to Business Associates and Other Contractors</i>	191
Appendix B: Forms and Templates	193
<i>Certificate of Destruction (Internal Destruction only)</i>	193
<i>Directory of Information Protection Contacts</i>	194
<i>Employee/Department Compliance Audit Report</i>	195
<i>Information/Asset Destruction Authorization</i>	196
<i>Information Destruction Contractor Compliance Audit Report</i>	197
<i>Information Destruction Policy Violation Report</i>	198
<i>Information Destruction Program Awareness Acknowledgement</i>	199
Sources	200
Chapter 8: Commercial Information Destruction Operations	201
Operational Data Security And Compliance Procedures	202
Applicant/Employee Screening	202
<i>Legal Status/Eligibility for Employment</i>	202
<i>Individual Confidentiality Agreements</i>	202
<i>Pre-Employment Criminal Background Screening</i>	203
<i>Substance Abuse Detection/Recognition</i>	204
<i>Ongoing Criminal Screening</i>	204
<i>Operator's License</i>	205
Operational Security	205
<i>Written Policies and Procedures</i>	205
<i>Employee Acknowledgement of Policies and Procedures</i>	205
<i>Employee Data Security Breach Notification Procedure</i>	205
<i>Incident Response Procedure</i>	205
<i>Audit Preparedness</i>	206
<i>Employee Training</i>	206
<i>Use of Photo I.D. Badges</i>	206
<i>Use of Uniforms</i>	206
<i>Acceptance of Data Controller Information/Media</i>	206
<i>Control and Protection of Media</i>	206
<i>Vehicle Roadworthiness</i>	207
<i>Vehicle Security</i>	207
<i>Driver Communications</i>	207
<i>Location of Destruction Event</i>	207
<i>Secure Destruction Facility Access Control</i>	207
<i>Visitors Login Requirements</i>	207

Information Disposition

<i>Dedicated Secured Area</i>208
<i>Monitored Alarm</i>208
<i>Closed Circuit Image Capture and Retention</i>208
<i>Use of Collection Facilities</i>208
<i>Use of Transfer Processing Station</i>209
Media Destruction: Physical Destruction209
<i>Paper/Printed Media</i>209
<i>Micro Media</i>210
<i>Physical Destruction of Hard Drives</i>210
<i>Physical Destruction of Non-Media</i>210
<i>Destruction Time Frame</i>210
<i>Responsible Disposal of Destroyed Remains</i>210
<i>Transfer of Custody</i>211
Media Destruction: Electronic Media Erasure211
<i>Physical Destruction Capability</i>211
<i>Written Hard Drive Overwriting Procedures</i>211
<i>Written Degaussing Procedures</i>212
<i>Quality Control Procedures for Overwriting Magnetic Media</i>213
<i>Quality Control Procedures for Degaussing Magnetic Media</i>213
<i>Unique Identifier Tracking</i>214
<i>Identification of Processed Media</i>214
<i>Calibration of Degaussing Equipment</i>215
<i>Training of Degaussing Technicians</i>215
<i>Evaluation of Media on Suitability of Degaussing</i>215
<i>Periodic External Verification of Degaussing Process</i>215
<i>Responsible Disposal of Destroyed Remains</i>216
Organizational Requirements216
<i>Required Certification(s)</i>216
<i>Designation of Compliance Officer</i>216
<i>Organizational Data Security Breach Notification Procedure</i>216
<i>Records Retention</i>217
Appendices218
Appendix A: Logs and Forms218
<i>Employee Confidentiality Agreement</i>218
<i>Agreement For Responsible Disposal Of Destroyed Materials</i>219
<i>SAMPLE Operational Policy & Procedures Manual</i>220
<i>Client Data Risk Incident Report</i>221
<i>NAID Certification Program Screen Changing Log</i>222
<i>NAID Certification Program Visitor Log</i>222

Appendix B: Secure Destruction Operations Safety 223

 1. *Scope* 223

 2. *Referenced Documents* 224

 3. *Terminology* 227

 4. *Significance and Use* 236

 5. *Design, Manufacture, Reconstruction, and Modification*. 237

 6. *Instructions for Operations and Maintenance* 238

 7. *Operational Requirements* 239

 8. *Mobile Equipment Safeguards and Features* 245

 9. *Safety Program and Training* 253

Sources 256

Chapter 9: Glossary of Terms 257

Index. 273