8. ORGANIZATIONAL ASSET MANAGEMENT

8.1 ESTABLISH RESPONSIBILITY FOR CORPORATE ASSETS

GOAL	To protect assets associated with information and information processing facilities.
MEMO	Define protection responsibilities for assets associated with your information and information processing facilities.

8.1.1 COMPILE AN INVENTORY OF ASSETS ASSOCIATED WITH INFORMATION

1	CTRL	Identify all assets associated with your organization's information and information processing facilities.	TODO	DONE	N/A	
2	CTRL	Compile an inventory of all assets associated with your information and information processing facilities.	TODO	DONE	N/A	
3	CTRL	Maintain an inventory of all assets associated with your information and information processing facilities.	TODO	DONE	N/A	
4	GUIDE	Use information lifecycle stages to identify assets.	TODO	DONE	N/A	
5	GUIDE	Identify assets used to create information.	TODO	DONE	N/A	
6	GUIDE	Identify assets used to process information.	TODO	DONE	N/A	
7	GUIDE	Identify assets used to store information.	TODO	DONE	N/A	
8	GUIDE	Identify assets used to transmit information.	TODO	DONE	N/A	
9	GUIDE	Identify assets used to delete information.	TODO	DONE	N/A	
10	GUIDE	Identify assets used to destroy information.	TODO	DONE	N/A	
11	GUIDE	Establish an inventory of information oriented assets.	TODO	DONE	N/A	
12	GUIDE	Classify each identified information oriented asset (8.2).	TODO	DONE	N/A	
13	GUIDE	Assign ownership to each information oriented asset (8.1.2).	TODO	DONE	N/A	
14	GUIDE	Align your inventory of assets with other inventories.	TODO	DONE	N/A	
15	GUIDE	Document your organization's inventory of assets.	TODO	DONE	N/A	
16	GUIDE	Store your documents in dedicated inventories.	TODO	DONE	N/A	
17	GUIDE	Specify the importance of each identified asset.	TODO	DONE	N/A	
18	GUIDE	Maintain your organization's inventory of assets.	TODO	DONE	N/A	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

19	GUIDE	Make sure that your asset inventory is accurate.	TODO	DONE	N/A	
20	GUIDE	Make sure that your asset inventory is up-to-date.	TODO	DONE	N/A	
21	GUIDE	Make sure that your inventory is internally consistent.	TODO	DONE	N/A	
22	NOTE	Assets cannot be properly protected unless you've previously identified and listed the assets that should be protected.				
23	NOTE	A complete inventory of information assets may also be required for health, safety, insurance, or financial reasons.				
24	NOTE	Also see ISO IEC 27005 for examples of the kinds of information oriented assets that ought to be protected.				
8.1.2 SELECT OWNERS FOR ALL ASSETS ASSOCIATED WITH YOUR INFORMATION						
25	**CTRL**	Select owners for assets associated with your information and information processing facilities.	TODO	DONE	N/A	
26	GUIDE	Establish a process to assign owners to all relevant assets.	TODO	DONE	N/A	
27	GUIDE	Make owners responsible for assets throughout asset lifecycles.	TODO	DONE	N/A	
28	GUIDE	Ask owners to define asset access restrictions and controls.	TODO	DONE	N/A	
29	GUIDE	Ask owners to manage their information oriented assets.	TODO	DONE	N/A	
30	GUIDE	Ask owners to ensure that assets are properly classified.	TODO	DONE	N/A	
31	GUIDE	Ask owners to ensure that assets are properly inventoried.	TODO	DONE	N/A	
32	GUIDE	Ask owners to ensure that assets are properly protected.	TODO	DONE	N/A	
33	GUIDE	Ask owners to ensure that assets are properly disposed of.	TODO	DONE	N/A	
34	GUIDE	Ask owners to ensure that assets are properly deleted.	TODO	DONE	N/A	
35	GUIDE	Ask owners to ensure that assets are properly destroyed.	TODO	DONE	N/A	
36	GUIDE	Ask owners to periodically review asset security practices.	TODO	DONE	N/A	
37	GUIDE	Ask owners to periodically review asset classifications.	TODO	DONE	N/A	
38	GUIDE	Ask owners to periodically review access restrictions.	TODO	DONE	N/A	
39	GUIDE	Ask owners to consider access control policies.	TODO	DONE	N/A	
40	GUIDE	Allocate ownership to people responsible for asset lifecycles.	TODO	DONE	N/A	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

41	GUIDE	Assign asset ownership when assets are created or acquired.	TODO	DONE	N/A	
42	NOTE	Asset owners do not actually "own" assets in the legal sense of the word, nor do they have any property rights to the asset.				
43	NOTE	An asset owner can be either a person or some other entity and should be responsible for the entire lifecycle of the asset.				
44	NOTE	While routine asset management tasks can be delegated, responsibility for the asset should remain with the asset owner.				
45	NOTE	When assets act together to provide a service, owners should be responsible for both the service and the underlying assets.				
8.1.3 PREPARE ACCEPTABLE USE RULES FOR ASSETS ASSOCIATED WITH INFORMATION						
46	**CTRL**	Define and document rules that clarify acceptable use of information.	TODO	DONE	N/A	
47	**CTRL**	Implement rules that clarify the acceptable use of information.	TODO	DONE	N/A	
48	**CTRL**	Define and document rules that clarify the acceptable use of assets associated with information and information processing facilities.	TODO	DONE	N/A	
49	**CTRL**	Implement rules that clarify the acceptable use of assets related to information and information processing facilities.	TODO	DONE	N/A	
50	GUIDE	Tell people about security requirements before allowing access.	TODO	DONE	N/A	
51	GUIDE	Make employees aware of information security requirements.	TODO	DONE	N/A	
52	GUIDE	Make third parties aware of information security requirements.	TODO	DONE	N/A	
53	GUIDE	Make people responsible for their use of facilities and resources.	TODO	DONE	N/A	
54	GUIDE	Hold people responsible even when they delegate use to others.	TODO	DONE	N/A	
8.1.4 RETURN ALL ASSETS ASSOCIATED WITH INFORMATION UPON TERMINATION						
55	**CTRL**	Make sure that all *employees* return all corporate assets associated with information and information processing facilities when their employment is terminated.	TODO	DONE	N/A	
56	**CTRL**	Make sure that all *external users* return all corporate assets associated with information and information processing facilities when their contract or agreement is terminated.	TODO	DONE	N/A	
57	GUIDE	Make the return of assets part of a formal termination process.	TODO	DONE	N/A	
58	GUIDE	Ask people to return physical and electronic assets at termination.	TODO	DONE	N/A	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

59	GUIDE	Protect company information on equipment of terminated users.	TODO	DONE	N/A	
60	GUIDE	Protect information on equipment sold to terminated users.	TODO	DONE	N/A	
61	GUIDE	Transfer information from equipment sold to terminated users.	TODO	DONE	N/A	
62	GUIDE	Make sure that all relevant information is securely erased.	TODO	DONE	N/A	
63	GUIDE	Protect information on terminated user's personal equipment.	TODO	DONE	N/A	
64	GUIDE	Transfer information from former user's personal equipment.	TODO	DONE	N/A	
65	GUIDE	Make sure that company information is securely erased.	TODO	DONE	N/A	
66	GUIDE	Preserve the knowledge that personnel have before they leave.	TODO	DONE	N/A	
67	GUIDE	Document all relevant knowledge before your personnel leave.	TODO	DONE	N/A	
68	GUIDE	Transfer knowledge to the company before personnel leave.	TODO	DONE	N/A	
69	GUIDE	Control unauthorized copying during notice period of termination.	TODO	DONE	N/A	
70	GUIDE	Prevent terminated employees from copying your information.	TODO	DONE	N/A	
71	GUIDE	Prevent terminated contractors from copying your information.	TODO	DONE	N/A	

8.2 DEVELOP AN INFORMATION CLASSIFICATION SCHEME

GOAL	To provide an appropriate level of protection for your organization's information.
MEMO	Your level of protection should reflect how important the information is to your organization.

8.2.1 CLASSIFY YOUR ORGANIZATION'S INFORMATION

72	CTRL	Adopt an information classification scheme.	TODO	DONE	N/A	
73	CTRL	Classify information according to the kinds of legal requirements that must be met.	TODO	DONE	N/A	
74	CTRL	Classify information according to how sensitive it is to unauthorized disclosure or modification.	TODO	DONE	N/A	
75	CTRL	Classify your information according to how valuable it is to your organization.	TODO	DONE	N/A	
76	CTRL	Classify information according to how critical it is.	TODO	DONE	N/A	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

8. ORGANIZATIONAL ASSET MANAGEMENT

77	GUIDE	Create an effective information classification scheme.	TODO	DONE	N/A	
78	GUIDE	Ensure that the scheme meets all legal requirements.	TODO	DONE	N/A	
79	GUIDE	Ensure that the scheme follows your access control policy (9.1.1).	TODO	DONE	N/A	
80	GUIDE	Ensure that the scheme addresses your unique business needs.	TODO	DONE	N/A	
81	GUIDE	Ensure that your scheme allows you to share information.	TODO	DONE	N/A	
82	GUIDE	Ensure that your scheme allows you to restrict access.	TODO	DONE	N/A	
83	GUIDE	Consider also classifying assets used to manage information.	TODO	DONE	N/A	
84	GUIDE	Consider also classifying assets used to store information.	TODO	DONE	N/A	
85	GUIDE	Consider also classifying assets used to process information.	TODO	DONE	N/A	
86	GUIDE	Consider also classifying assets used to handle information.	TODO	DONE	N/A	
87	GUIDE	Consider also classifying assets used to protect information.	TODO	DONE	N/A	
88	GUIDE	Design your organization's information classification scheme.	TODO	DONE	N/A	
89	GUIDE	Make owners of assets accountable for their classification.	TODO	DONE	N/A	
90	GUIDE	Ensure that assets and information can be consistently classified.	TODO	DONE	N/A	
91	GUIDE	Ensure that classifiers share a common understanding.	TODO	DONE	N/A	
92	GUIDE	Ensure that each classification level has an intuitive name.	TODO	DONE	N/A	
93	GUIDE	Ensure that everyone can do classifications in the same way.	TODO	DONE	N/A	
94	GUIDE	Ensure that protection requirements are widely understood.	TODO	DONE	N/A	
95	GUIDE	Ensure that confidentiality requirements are understood.	TODO	DONE	N/A	
96	GUIDE	Ensure that availability requirements are understood.	TODO	DONE	N/A	
97	GUIDE	Ensure that integrity requirements are understood.	TODO	DONE	N/A	
98	GUIDE	Integrate your classification scheme into your other processes.	TODO	DONE	N/A	
99	GUIDE	Implement your organization's classification scheme.	TODO	DONE	N/A	
100	GUIDE	Classify all forms of information in order to safeguard it.	TODO	DONE	N/A	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

8. ORGANIZATIONAL ASSET MANAGEMENT

101	GUIDE	Classify information according to how important it is.	TODO	DONE	N/A	
102	GUIDE	Classify information according to how valuable it is.	TODO	DONE	N/A	
103	GUIDE	Classify information according to how sensitive it is.	TODO	DONE	N/A	
104	GUIDE	Classify information according to how critical it is.	TODO	DONE	N/A	
105	GUIDE	Classify information according to how much protection it needs.	TODO	DONE	N/A	
106	GUIDE	Classify information according to how confidential it must be.	TODO	DONE	N/A	
107	GUIDE	Classify information according to how available it must be.	TODO	DONE	N/A	
108	GUIDE	Classify assets used to manage information.	TODO	DONE	N/A	
109	GUIDE	Classify assets used to store information.	TODO	DONE	N/A	
110	GUIDE	Classify assets used to process information.	TODO	DONE	N/A	
111	GUIDE	Classify assets used to handle information.	TODO	DONE	N/A	
112	GUIDE	Classify assets used to protect information.	TODO	DONE	N/A	
113	GUIDE	Review classifications whenever needs or requirements change.	TODO	DONE	N/A	
114	GUIDE	Establish criteria for reviewing classifications during their lifecycle.	TODO	DONE	N/A	
115	GUIDE	Assess the level of protection that classifiers are assigning.	TODO	DONE	N/A	
116	GUIDE	Analyze changes in your organization’s requirements.	TODO	DONE	N/A	
117	GUIDE	Examine changes in confidentiality requirements.	TODO	DONE	N/A	
118	GUIDE	Examine changes in availability requirements.	TODO	DONE	N/A	
119	GUIDE	Examine changes in integrity requirements.	TODO	DONE	N/A	
120	GUIDE	Analyze changes in the status of information.	TODO	DONE	N/A	
121	GUIDE	See if the value of your information has changed.	TODO	DONE	N/A	
122	GUIDE	See if the criticality of your information has changed.	TODO	DONE	N/A	
123	GUIDE	See if the sensitivity of your information has changed.	TODO	DONE	N/A	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

124	GUIDE	Update your classifications throughout their lifecycle.	TODO	DONE	N/A	
125	GUIDE	Update classifications to reflect changes in requirements.	TODO	DONE	N/A	
126	GUIDE	Accommodate changes in confidentiality requirements.	TODO	DONE	N/A	
127	GUIDE	Accommodate changes in availability requirements.	TODO	DONE	N/A	
128	GUIDE	Accommodate changes in integrity requirements.	TODO	DONE	N/A	
129	GUIDE	Update classifications to reflect changes in information.	TODO	DONE	N/A	
130	GUIDE	Update classifications to accommodate changes in value.	TODO	DONE	N/A	
131	GUIDE	Update classifications to accommodate changes in criticality.	TODO	DONE	N/A	
132	GUIDE	Update classifications to accommodate changes in sensitivity.	TODO	DONE	N/A	
133	NOTE	Group information into categories (classifications) that have similar protection needs and requirements.				
134	NOTE	For each category, develop an information security procedure that applies to all the information in that category.				
135	NOTE	Use your categories to tell people how to handle and how to protect the information in each particular category.				
136	NOTE	Use categories to avoid having to carry out case-by-case risk assessments and to avoid having to design special controls.				
137	NOTE	Information sometimes needs to be reclassified because it's no longer sensitive or critical (e.g., after it's been made public).				
138	NOTE	Because of this, care should be taken to review classifications and to reclassify information whenever its status changes.				
139	NOTE	This is important because over-classification can be expensive while under-classification can be dangerous.				
8.2.2 ESTABLISH INFORMATION LABELING PROCEDURES						
140	CTRL	Develop an appropriate set of information labeling procedures in accordance with your information classification scheme.	TODO	DONE	N/A	
141	CTRL	Implement your information labeling procedures.	TODO	DONE	N/A	
142	GUIDE	Prepare an effective set of information labeling procedures.	TODO	DONE	N/A	
143	GUIDE	Prepare procedures for both information and related assets.	TODO	DONE	N/A	
144	GUIDE	Make sure that they apply to both physical and electronic assets.	TODO	DONE	N/A	
145	GUIDE	Make sure that they explain where and how labels are attached.	TODO	DONE	N/A	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

146	GUIDE	Consider how information is accessed and assets are handled.	TODO	DONE	N/A	
147	GUIDE	Consider types of media when you prepare procedures.	TODO	DONE	N/A	
148	GUIDE	Make sure that they clarify when labeling should not be done.	TODO	DONE	N/A	
149	GUIDE	Prepare labels that work for both physical and electronic assets.	TODO	DONE	N/A	
150	GUIDE	Make sure that they apply your classification scheme (see 8.2.1.).	TODO	DONE	N/A	
151	GUIDE	Make sure that they are simple to use and easy to recognize.	TODO	DONE	N/A	
152	GUIDE	Teach employees and contractors about your labeling procedures.	TODO	DONE	N/A	
153	GUIDE	Ask employees and contractors to use your labeling procedures.	TODO	DONE	N/A	
154	GUIDE	Attach appropriate labels to both information and related assets.	TODO	DONE	N/A	
155	GUIDE	Attach labels to information classified as sensitive or critical.	TODO	DONE	N/A	
156	NOTE	Information sharing arrangements usually expect organizations to use labels to classify information.				
157	NOTE	Common types of labels include physical stickers and metadata (data that describes other data).				
158	NOTE	Be careful about how you manage information and assets that are labeled as secret, sensitive, or confidential (for example).				
159	NOTE	Classified information and physical assets are easier to identify and therefore easier for people to steal or misuse.				
8.2.3 DEVELOP ASSET HANDLING PROCEDURES						
160	CTRL	Develop procedures for handling assets associated with your information and information processing facilities.	TODO	DONE	N/A	
161	CTRL	Make sure that your asset handling procedures respect and reflect how you classify information (see 8.2.1).	TODO	DONE	N/A	
162	CTRL	Implement your asset handling procedures.	TODO	DONE	N/A	
163	GUIDE	Design procedures for handling classified information (see 8.2.1).	TODO	DONE	N/A	
164	GUIDE	Ensure that information is handled according to its classification.	TODO	DONE	N/A	
165	GUIDE	Ensure that it is protected according to its classification.	TODO	DONE	N/A	
166	GUIDE	Ensure that it is protected when shared with outsiders.	TODO	DONE	N/A	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

167	GUIDE	Establish security agreements with other organizations.	TODO	DONE	N/A	
168	GUIDE	Establish procedures to control classified information.	TODO	DONE	N/A	
169	GUIDE	Clarify how your classifications should be interpreted.	TODO	DONE	N/A	
170	GUIDE	Clarify how others' classifications should be interpreted.	TODO	DONE	N/A	
171	GUIDE	Ensure that it is stored according to its classification.	TODO	DONE	N/A	
172	GUIDE	Ensure that it is processed according to its classification.	TODO	DONE	N/A	
173	GUIDE	Ensure that it is transmitted according to its classification.	TODO	DONE	N/A	
174	GUIDE	Ensure that it is copied according to its classification.	TODO	DONE	N/A	
175	GUIDE	Make sure copies get the same protection as originals.	TODO	DONE	N/A	
176	GUIDE	Ensure that it is accessed according to its classification.	TODO	DONE	N/A	
177	GUIDE	Design access restrictions for each level of classification.	TODO	DONE	N/A	
178	GUIDE	Ensure that restrictions meet protection requirements.	TODO	DONE	N/A	
179	GUIDE	Establish a formal record of authorized recipients of assets.	TODO	DONE	N/A	
180	GUIDE	Mark media copies for the attention of authorized recipients.	TODO	DONE	N/A	
181	GUIDE	Use asset handling procedures to manage information.	TODO	DONE	N/A	
182	GUIDE	Protect information according to how it is classified.	TODO	DONE	N/A	
183	GUIDE	Store information according to how it is classified.	TODO	DONE	N/A	
184	GUIDE	Store IT assets according to manufacturers' specifications.	TODO	DONE	N/A	
185	GUIDE	Process information according to how it is classified.	TODO	DONE	N/A	
186	GUIDE	Transmit information according to how it is classified.	TODO	DONE	N/A	
187	GUIDE	Specify who the authorized recipient should be.	TODO	DONE	N/A	
188	GUIDE	Copy information according to how it is classified.	TODO	DONE	N/A	
189	GUIDE	Access information according to how it is classified.	TODO	DONE	N/A	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

8.3 CONTROL HOW PHYSICAL MEDIA ARE HANDLED

GOAL	To protect information by preventing unauthorized disclosure, modification, removal, or destruction of storage media.					
8.3.1 MANAGE REMOVABLE MEDIA						
190	CTRL	Establish procedures for managing removable media.	TODO	DONE	N/A	
191	CTRL	Make sure that your media management procedures respect and reflect how you classify information.	TODO	DONE	N/A	
192	CTRL	Implement your removable media management procedures.	TODO	DONE	N/A	
193	GUIDE	Develop removable media management procedures.	TODO	DONE	N/A	
194	GUIDE	Control the use and management of removable media.	TODO	DONE	N/A	
195	GUIDE	Reduce the risk of data loss by registering removable media.	TODO	DONE	N/A	
196	GUIDE	Enable media drives only if you have a good reason to do so.	TODO	DONE	N/A	
197	GUIDE	Monitor the transfer of information to removable media.	TODO	DONE	N/A	
198	GUIDE	Control the methods used to protect removable media.	TODO	DONE	N/A	
199	GUIDE	Use cryptographic techniques to protect data on media.	TODO	DONE	N/A	
200	GUIDE	Prevent data degradation by transferring it to fresh media.	TODO	DONE	N/A	
201	GUIDE	Make contents unrecoverable when it is no longer needed.	TODO	DONE	N/A	
202	GUIDE	Control the methods used to store removable media.	TODO	DONE	N/A	
203	GUIDE	Store valuable data on separate media to prevent losing it.	TODO	DONE	N/A	
204	GUIDE	Protect removable media by creating multiple copies of it.	TODO	DONE	N/A	
205	GUIDE	Store removable media in a safe and secure environment.	TODO	DONE	N/A	
206	GUIDE	Follow your manufacturers' media storage specifications.	TODO	DONE	N/A	
207	GUIDE	Control the removal of media from your organization's premises.	TODO	DONE	N/A	
208	GUIDE	Establish a system of authorization to control media removals.	TODO	DONE	N/A	
209	GUIDE	Create levels of authorization to control all media removals.	TODO	DONE	N/A	
210	GUIDE	Document authorization levels to control media removals.	TODO	DONE	N/A	
211	GUIDE	Keep records and maintain an audit trail of media removals.	TODO	DONE	N/A	
212	GUIDE	Document your removable media management procedures.	TODO	DONE	N/A	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

8.3.2 MANAGE THE DISPOSAL OF MEDIA						
213	CTRL	Establish formal procedures to securely dispose of storage media that are no longer required.	TODO	DONE	N/A	
214	CTRL	Apply your storage media disposal procedures.	TODO	DONE	N/A	
215	GUIDE	Establish procedures to manage the secure disposal of media.	TODO	DONE	N/A	
216	GUIDE	Develop procedures to identify media that require disposal.	TODO	DONE	N/A	
217	GUIDE	Figure out how to identify items that require secure disposal.	TODO	DONE	N/A	
218	GUIDE	Select confidential items that require secure disposal.	TODO	DONE	N/A	
219	GUIDE	Use secure disposals to reduce the risk of damaging leaks.	TODO	DONE	N/A	
220	GUIDE	Select data that may become sensitive as you aggregate it.	TODO	DONE	N/A	
221	GUIDE	Consider the “aggregation effect” as you identify items.	TODO	DONE	N/A	
222	GUIDE	Develop procedures to securely dispose of selected media.	TODO	DONE	N/A	
223	GUIDE	Develop procedures to control how information is destroyed.	TODO	DONE	N/A	
224	GUIDE	Consider developing secure incineration procedures.	TODO	DONE	N/A	
225	GUIDE	Consider developing secure shredding procedures.	TODO	DONE	N/A	
226	GUIDE	Consider developing secure erasure procedures.	TODO	DONE	N/A	
227	GUIDE	Develop procedures to control the use of disposal companies.	TODO	DONE	N/A	
228	GUIDE	Make sure that disposal companies have suitable experience.	TODO	DONE	N/A	
229	GUIDE	Make sure that disposal companies have adequate controls.	TODO	DONE	N/A	
230	GUIDE	Develop procedures to control media disposal records.	TODO	DONE	N/A	
231	GUIDE	Maintain an audit trail by logging the disposal of sensitive items.	TODO	DONE	N/A	
232	GUIDE	Use your procedures to securely dispose of selected media.	TODO	DONE	N/A	
233	GUIDE	Consider the sensitivity of items when you dispose of media.	TODO	DONE	N/A	
234	GUIDE	Consider securely disposing all items not just sensitive ones.	TODO	DONE	N/A	
235	NOTE	Use a risk assessment to decide what to do with damaged devices that contain sensitive data.				
236	NOTE	Decide whether or not damaged devices should be repaired, destroyed, or discarded (see 11.2.7).				

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

8.3.3 MANAGE THE TRANSFER OF MEDIA						
237	CTRL	Protect physical media while it is being transported whenever it contains information that must be protected.	TODO	DONE	N/A	
238	CTRL	Prevent unauthorized access to media during transport.	TODO	DONE	N/A	
239	CTRL	Prevent the corruption of media during transport.	TODO	DONE	N/A	
240	CTRL	Prevent the misuse of media during transport.	TODO	DONE	N/A	
241	GUIDE	Use reliable methods to transport physical media.	TODO	DONE	N/A	
242	GUIDE	Use dependable couriers to transport physical media.	TODO	DONE	N/A	
243	GUIDE	Develop procedures to verify the identity of couriers.	TODO	DONE	N/A	
244	GUIDE	Ask management to establish a list of authorized couriers.	TODO	DONE	N/A	
245	GUIDE	Use adequate packaging to protect media during transit.	TODO	DONE	N/A	
246	GUIDE	Use packaging that meets manufacturers' specifications.	TODO	DONE	N/A	
247	GUIDE	Use packaging that protects contents from physical damage.	TODO	DONE	N/A	
248	GUIDE	Prevent exposure to environmental hazards and threats.	TODO	DONE	N/A	
249	GUIDE	Prevent exposure to electromagnetic fields.	TODO	DONE	N/A	
250	GUIDE	Prevent exposure to heat and moisture.	TODO	DONE	N/A	
251	GUIDE	Keep a log or establish a record of media transfers.	TODO	DONE	N/A	
252	GUIDE	Identify the information and media being transferred.	TODO	DONE	N/A	
253	GUIDE	Specify the methods used to protect media during transit.	TODO	DONE	N/A	
254	GUIDE	Establish a record of media delivery and arrival times and dates.	TODO	DONE	N/A	
255	NOTE	Consider adding additional physical protection whenever unencrypted information is transported.				
256	NOTE	In the context of this section, the term "physical media" also includes paper documents.				

Consider each task on the left and select an appropriate response. If you haven't done it and you feel it needs to be done, select *TODO*. Select *TODO* if the task addresses one of your information security risks or needs. If you've already done the task, select *DONE*. If the task is not applicable in your situation or it does not address your security risks and needs, then answer N/A. Also, use the space on the right to record your notes and comments, and in the spaces below please enter the name and location of your organization, who completed this page, who reviewed it, and the dates.

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

