Risk Check

	Risk Evaluation					Control		Risk Evaluation after Control		
#	Threat	Comments on Threat	Vulnerability	Comments on Vulnerability	Total Risk	Control Contents	References	Threat	Vulnerability	Total Risk
							Rule book or Resi	dual Risk List		
1										
2										
3										
4										
5	2: Middle	Overall	2: Middle		2: High (15pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
6	2: Middle	Overall	2: Middle		2: High (15pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
7	2: Middle	Overall	2: Middle		2: High (15pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
8	2: Middle	Overall	2: Middle		2: High (15pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
9										
10	2: Middle	Staff errors to treat confidential information	2: Middle		2: High (15pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
11										
12										
13	2: Middle	Staff errors to treat confidential information	2: Middle		2: High (15pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
14										
15										
16										
17										
18										
19										
20										
21										
22										
23										
24										
25										
26										
27	2: Middle	Forced entry, unauthorized access	2: Middle		2: High (12pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
28	2: Middle	Forced entry, unauthorized access	2: Middle		2: High (12pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
29	2: Middle	Forced entry, unauthorized access	2: Middle		2: High (12pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
30	2: Middle	Forced entry, unauthorized access	2: Middle		2: High (12pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
31	2: Middle	Forced entry, unauthorized access	2: Middle		2: High (12pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
32	2: Middle	Information leak	2: Middle		2: High (12pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
33										
34	2: Middle	Forced entry, unauthorized access	2: Middle		2: High (12pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
35										
36	2: Middle	Forced entry, unauthorized access	2: Middle		2: High (12pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
37	2: Middle	Information leak	2: Middle		2: High (12pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
38										
39	2: Middle	Forced entry, unauthorized access	2: Middle		2: High (12pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
40	2: Middle	Forced entry, unauthorized access	2: Middle		2: High (12pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
41										
42										
43	2: Middle	Staff errors to treat confidential information	2: Middle		2: High (12pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
44	2: Middle	Forced entry, unauthorized access	2: Middle		2: High (12pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
45	2: Middle	Information leak	2: Middle		2: High (12pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
46										
47	2: Middle	Staff errors to treat confidential information	2: Middle		2: High (9pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
48	2: Middle	Forced entry, unauthorized access	2: Middle		2: High (9pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
49	2: Middle	Information leak	2: Middle		2: High (9pt)	Implement Rules	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)

Risk Check

	Risk Evaluation					Control		Risk Evaluation after Control		
#	Threat	Comments on Threat	Vulnerability	Comments on Vulnerability	Total Risk	Control Contents	References	Threat	Vulnerability	Total Risk
50										
51										
52	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
53	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
54	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
55	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
56	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
57	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
58	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
59	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
60	2: Middle	Circuit breaker down	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
61	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
62										
63	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
64										
65	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
66	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
67										
68	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
69										
70	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
71	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
72	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
73	2: Middle	Unauthorized access, falsification	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
74	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
75	2: Middle	falsification	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
76	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)

Risk Check

	Risk Evaluation					Control		Risk Evaluation after Control		
#	Threat	Comments on Threat	Vulnerability	Comments on Vulnerability	Total Risk	Control Contents	References	Threat	Vulnerability	Total Risk
77										
78										
79										
80	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
81	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
82	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
83	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
84	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
85	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
86										
87	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
88										
89	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
90	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
91										
92	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
93	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
94										
95										
96	2: Middle	Staff errors to treat confidential information	3: Middle		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
97	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
98	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
99										
100	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (8pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
101	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (8pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
102	2: Middle	Information leak	3: Middle		2: High (8pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
103										
104										
105	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (8pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
106	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (8pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
107	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (8pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
108	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (8pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
109	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (8pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
110	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (8pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
111	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (8pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
112	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (8pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
113	2: Middle	Circuit breaker down	3: Middle		2: High (8pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
114	2: Middle	Information leak	3: Middle		2: High (8pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
115										
116	2: Middle	Information leak	3: Middle		2: High (8pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
117										
118	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (8pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
119	2: Middle	Information leak	3: Middle		2: High (8pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
120										
121	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (8pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
122										
123	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (8pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
124	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (8pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
125	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (8pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
126	2: Middle	Unauthorized access, falsification	3: Middle		2: High (8pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
127	2: Middle	Information leak	3: Middle		2: High (8pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
128	2: Middle	Falsification	3: Middle		2: High (8pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
129	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (8pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)

Risk Check

	Risk Evaluation				Control		Risk Evaluation after Control		
#	Threat	Comments on Threat	Vulnerability	Comments on Vulnerability	Total Risk	Control Contents	References	Threat	Vulnerability	Total Risk
130										
131										
132	2: Middle	Entry for external hackers	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
133	2: Middle	Continuous unauthorized access	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
134	2: Middle	Continuous unauthorized access	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
135	2: Middle	Circuit breaker down	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
136										
137	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
138	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
139	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
140	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
141	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
142	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
143	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
144	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
145	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
146	2: Middle	Data damage by software flaw and malfunction	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
147	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
148	2: Middle	Service unavailable for a long time	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
149	2: Middle	Continuous unauthorized access	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
150	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
151	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
152	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
153	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
154	2: Middle	Continuous unauthorized access	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
155	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
156	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
157	2: Middle	Circuit breaker down	3: Middle		2: High (6pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)

Risk Check

	Risk Evaluation					Control		Risk Evaluation after Control		
#	Threat	Comments on Threat	Vulnerability	Comments on Vulnerability	Total Risk	Control Contents	References	Threat	Vulnerability	Total Risk
158										
159										
160	2: Middle	Entry for external hackers	3: Middle		2: High (12pt)	Suspended until PAIS integrating GAIS		2: Middle	3: Middle	2: High (12pt)
161	2: Middle	Continuous unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
162	2: Middle	Continuous unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
163	2: Middle	Circuit breaker down	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
164										
165	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
166	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
167	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
168	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
169	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
170	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
171	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
172	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
173	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
174	2: Middle	Data damage by software flaw and malfunction	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
175	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
176	2: Middle	Service unavailable for a long time	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
177	2: Middle	Continuous unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
178	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
179	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
180	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
181	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
182	2: Middle	Continuous unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
183	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
184	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
185	2: Middle	Circuit breaker down	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)

Risk Check

#	Risk Evaluation					Control		Risk Evaluation after Control		
	Threat	Comments on Threat	Vulnerability	Comments on Vulnerability	Total Risk	Control Contents	References	Threat	Vulnerability	Total Risk
186										
187										
188										
189	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
190	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
191	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
192	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
193	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
194	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
195										
196	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
197										
198	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
199	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
200										
201	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
202	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
203										
204										
205	2: Middle	Staff errors to treat confidential information	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
206	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
207	2: Middle	Information leak	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
208										
209	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
210	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
211	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
212										
213										
214	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
215	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
216	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
217	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
218	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
219	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
220	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
221	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
222	2: Middle	Circuit breaker down	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
223	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
224										
225	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
226										
227	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
228	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
229										
230	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
231										
232	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
233	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
234	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
235	2: Middle	Unauthorized access, falsification	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
236	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
237	2: Middle	falsification	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
238	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
239										
240										

Risk Check

	Risk Evaluation					Control		Risk Evaluation after Control		
I	Threat	Comments on Threat	Vulnarability	Comments on Vulnarability	Total Risk	Control Contents	References	Threat	Vulnarability	Total Risk
241							Rule book or Risk assessment plan			
242										
243										
244										
245										
246										
247										
248										
249										
250										
251										
252										
253										
254										
255										
256										
257										
258										
259										
260										
261										

Risk Check

#	Risk Evaluation					Control		Risk Evaluation after Control		
	Threat	Comments on Threat	Vulnerability	Comments on Vulnerability	Total Risk	Control Contents	References	Threat	Vulnerability	Total Risk
262										
263										
264										
265	1: Low	Forced entry, unauthorized access	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
266	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
267	2: Middle	Forced entry, unauthorized access	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
268	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
269	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
270	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
271										
272	3: High	Forced entry, unauthorized access	4: High		2: High (20pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
273										
274	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
275	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
276										
277	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
278	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
279										
280										
281	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
282	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
283	2: Middle	Information leak	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
284										
285	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
286	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
287	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
288										
289										
290	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
291	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
292	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
293	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
294	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
295	1: Low	Unauthorized access, falsification, malfunction	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
296	1: Low	Unauthorized access, falsification, malfunction	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
297	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
298	2: Middle	Circuit breaker down	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
299	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
300										
30	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
302										
303	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
304	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
305										
306	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
307										
308	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
309	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
310	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
311	3: High	Unauthorized access, falsification	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
312	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
313	2: Middle	falsification	4: High		2: High (16pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
314	3: High	Software flaw, malfunction, malware	4: High		2: High (20pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)

Risk Check

1

#	Risk Evaluation					Control		Risk Evaluation after Control		
	Threat	Comments on Threat	Vulnerability	Comments on Vulnerability	Total Risk	Control Contents	References	Threat	Vulnerability	Total Risk
315										
316										
317										
318	2: Middle	Forced entry, unauthorized access	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
319	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
320	2: Middle	Forced entry, unauthorized access	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
321	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
322	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
323	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
324										
325	3: High	Forced entry, unauthorized access	4: High		2: High (20pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
326										
327	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
328	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
329										
330	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
331	2: Middle	Forced entry, unauthorized access	2: Fair		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
332										
333										
334	3: High	Staff errors to treat confidential information	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
335	3: High	Forced entry, unauthorized access	4: High		2: High (20pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
336	3: High	Information leak	4: High		2: High (20pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
337										
338	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
339	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
340	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
341										
342										
343	2: Middle	Unauthorized access, falsification, malfunction	2: Fair		2: High (8pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
344	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
345	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
346	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
347	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
348	1: Low	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
349	1: Low	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
350	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
351	2: Middle	Circuit breaker down	4: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
352	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
353										
354	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
355										
356	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
357	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
358										
359	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
360										
361	1: Low	Software flaw, malfunction, malware	2: Fair		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
362	1: Low	Software flaw, malfunction, malware	2: Fair		1: Low (0pt)	Implement Rule and Procedures	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
363	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
364	3: High	Unauthorized access, falsification	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
365	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
366	2: Middle	falsification	4: High		2: High (16pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
367	3: High	Software flaw, malfunction, malware	4: High		2: High (20pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)

Risk Check

#	Risk Evaluation					Control		Risk Evaluation after Control		
	Threat	Comments on Threat	Vulnerability	Comments on Vulnerability	Total Risk	Control Contents	References	Threat	Vulnerability	Total Risk
368										
369										
370										
371	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
372	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
373	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
374	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
375	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
376	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
377										
378	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
379										
380	3: High	Forced entry, unauthorized access	3: Middle		2: High (15pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
381	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
382										
383	1: Low	Forced entry, unauthorized access	2: Fair		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
384	1: Low	Forced entry, unauthorized access	2: Fair		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
385										
386										
387	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
388	1: Low	Forced entry, unauthorized access	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
389	2: Middle	Information leak	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
390										
391	1: Low	Staff errors to treat confidential information	2: Fair		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
392	1: Low	Forced entry, unauthorized access	1: Low		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
393	2: Middle	Information leak	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
394										
395										
396	1: Low	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
397	1: Low	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
398	1: Low	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
399	1: Low	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
400	1: Low	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
401	1: Low	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
402	1: Low	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
403	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (15pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
404	2: Middle	Circuit breaker down	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
405	2: Middle	Information leak	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
406										
407	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
408										
409	2: Middle	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
410	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
411										
412	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
413										
414	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
415	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
416	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
417	3: High	Unauthorized access, falsification	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
418	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
419	1: Low	falsification	1: Low		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
420	2: Middle	Software flaw, malfunction, malware	4: High		2: High (16pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)

Risk Check

	Risk Evaluation					Control		Risk Evaluation after Control		
#	Threat	Comments on Threat	Vulnerability	Comments on Vulnerability	Total Risk	Control Contents	References	Threat	Vulnerability	Total Risk
512										
513										
514										
515	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
516	3: High	Forced entry, unauthorized access	3: Middle		2: High (15pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
517	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
518	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
519	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
520	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
521										
522	3: High	Forced entry, unauthorized access	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
523										
524	3: High	Forced entry, unauthorized access	3: Middle		2: High (15pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
525	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
526										
527	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
528	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
529										
530										
531	3: High	Staff errors to treat confidential information	3: Middle		2: High (15pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
532	3: High	Forced entry, unauthorized access	3: Middle		2: High (15pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
533	3: High	Information leak	3: Middle		2: High (15pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
534										
535	2: Middle	Staff errors to treat confidential information	3: Middle		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
536	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
537	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
538										
539										
540	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
541	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
542	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
543	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
544	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
545	1: Low	Unauthorized access, falsification, malfunction	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
546	1: Low	Unauthorized access, falsification, malfunction	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
547	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
548	2: Middle	Circuit breaker down	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
549	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
550										
551	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
552										
553	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
554	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
992										
555	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
557										
558	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
559	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
560	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
561	3: High	Unauthorized access, falsification	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
562	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
563	2: Middle	falsification	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
564	2: Middle	Software flaw, malfunction, malware	4: High		2: High (16pt)	Implement Rule and Procedures.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)

SECTION 5
Government Information Security Rule

- Drafted by Yusuke Tanaka, JICA Expert.
- Edited by ICT Security Management Technical Team (iSMTT).

1. Introduction

The Government Information Security Rule Book (GIS Rule Book) at NiDA is defined as NiDA implements the Government Information Security Management System (GISMS) under Information Security Management System Policy and the Government Information Security Management Manual (GISMS Manual).

2. Three Basic Rules to Secure Information

[Rule 1] Always consider whether you acquire, process or save confidential information. Do NOT expose information against any risks of leakage, falsification and inaccessibility.

[Rule 2] Lock up an office entrance, a cabinet and a desk drawer before walking away for any moment.

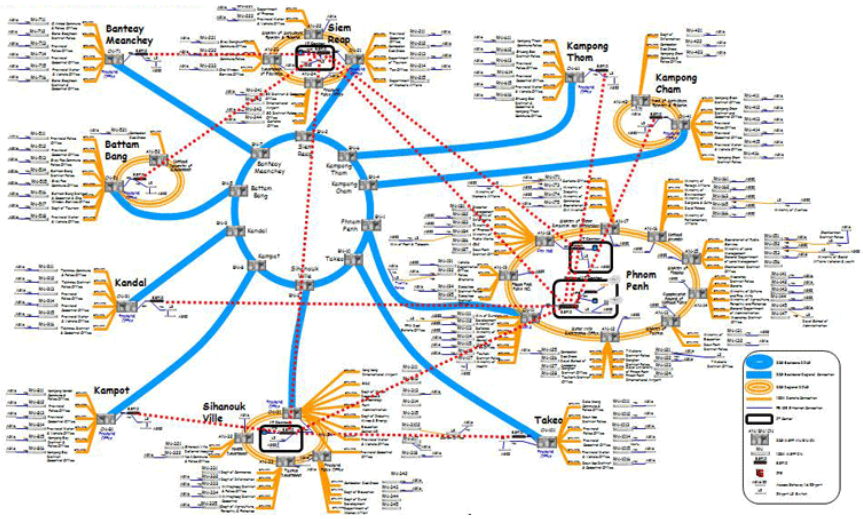
[Rule 3] Activate an auto-detection function of anti-virus software. Update a virus definition file at least weekly. Scan a storage device of your PC weekly and any external storage devices (e.g. FD, Memory Card/Stick and HDD) when to connect to your PC.

3. Scope

The GIS Rule Book covers National Information Communication Technology Development Authority (NiDA), which consists of the following departments; *General Administration, Infrastructure, Network, Enterprise, Content and Applications, Human Capacity Building and FOSS and Policy*. The GIS Rule Book also covers the following organizations under Secretary General; *Secretary General Office, Information Desk, Cambodia Computer Emergency Response Team, Singapore Operation Program, CISCO Training, and The Priority Management Group.*

From a network/system perspective, the GIS Rule Book covers client PC. The scope of GIS Rule Book will be extended to Servers and PAIS in the future.

NiDA has paid attention to develop the project Provincial Administration Information System (PAIS) and connect network system to all provinces.



(National Information Infrastructure Diagram)

4. Normative References, Terms and Definition

4.1. Normative References

The following referenced documents are indispensable for the application of this document.

1) ISO/ISE 27001: 2005 Information technology – Security techniques – Information security management systems – Requirements

2) The Government Information Security Management System Manual (GISMS Manual)

4.2. Terms and Definition

The followings are the terms and their definitions specifically used in GIS Rule Book.

Client PC:

It is a local PC as a type of desktop PC, laptop PC or mobile PC.

All other terms are referred to Terms and Definition in GISMS Manual or ISO/ISE 27001.

5. Information Security Organization

5.1. Information Security Organization Definition

NiDA sets the following information security roles and responsibilities.

Information Security Office (ISO):

It is set up at NiDA. It is responsible for implementing ISMS at NiDA. ISO members are CISO, IS Manager and IS In-charge, which are defined below.

Chief Information Security Officer (CISO):

One person is assigned at a ministry. He/she is also a member of Government Information Security Office (GISO), which is defined in GISMS.

Information Security Manager (IS Manager):

The role is assigned to an official by department. Its responsibilities are defined both in GISMS Manual and in GIS Rule Book.

Information Security In-charge (IS In-charge):

The role is assigned to an official also by department. Its responsibilities are defined in GIS Rule Book.

Official: All other employees of the in-scope organization.

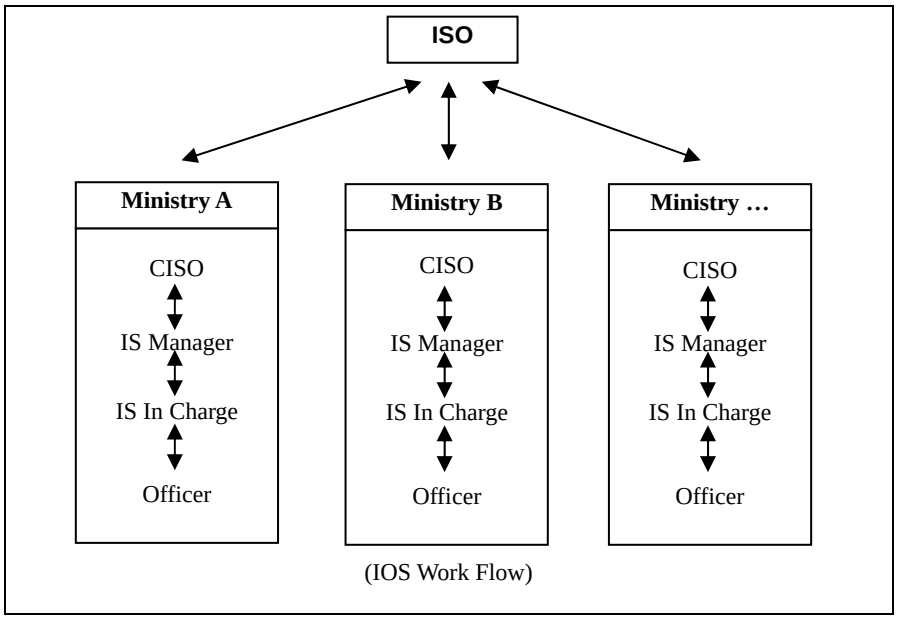
5.2. ISO Member List

ISO members will be assigned by the Secretary General of the National ICT Development Authority (NiDA).

5.3. Communication Route at Emergency

The reporting path is generally defined, from Officials to IS In-charge, IS In-charge to IS Manager, IS Manager to ISO/CISO. The instructing path is generally defined, from CISO/ISO to IS Manager, IS manager to IS In-charge, and IS In-charge to Officials in vice versa.

In the diagram is ISO work flow organization chart:



(IOS Work Flow)

6. Rule and Procedures

6.1. Information Classification

(a) Rule

(a1) Information used in a government business operation is classified into three categories.

1. General:
   Open information which goes public
2. Internal:
   Information used only in a government business operation
3. Confidential:
   Confidential among limited authorized people

(a2) Classify information when you acquire and it is highly recommended one is marked or labeled showing the information classification.

(a3) Always manage information carefully according to the classification.

(a4) Classify privacy information always as confidential.

(b) Procedure

(No procedure is applied for this section.)

6.2. People Security (To be defined in a future)

(a) Rule

(This section defines the security requirements of people matter such as the candidate qualification check in the hiring process, a job description related to information security matters, and the requirements at the termination of employment.)

6.3. Facility Security

6.3.1. Office Building and Room

(a) Rule

(a1) Define those who can enter the facility/room.
(a2) Implement an appropriate key system for an entrance of the facility/room.
(a3) Separate an office space and the other accessible common space.
(a4) Get outsiders with an insider attendant.
(a5) Record an entry and exit.
(a6) Keep records of courier service.

Suspension

(b) Procedure

(No procedure is applied for this section.)

6.3.2. Cabinet and Desk

(a) Rule

(a1) Store information assets with confidential information and lock up cabinets.

(b) Procedure

(No procedure is applied for this section.)

6.3.3. Fax Machine and Printer

(a) Rule

(a1) Dispose printed materials/faxed materials with care.
(a2) Keep record of faxing (sending/receiving).

(b) Procedure

(No procedure is applied for this section.)

6.4. Physical Information Security

6.4.1. Paper

(a) Rule

(a1) Always carefully identify confidential information within each paper/document.

(a2) Save confidential paper/documents in safe against unauthorized access.

(a3) Officials must burn disposing paper by themselves. Or use a paper shredder with disposing paper including confidential information.

(b) Procedure

(No procedure is applied for this section.)

6.4.2. Digital Archives (DVD/CD/FD/Tape)

(a) Rule

(a1) Always carefully identify confidential information within each archive.

(a2) Save confidential archives in safe against unauthorized access.

(a3) Scrap a media (Tape/FD/CD/DVD) physically.

(b) Procedure

(No procedure is applied for this section.)

6.5. Client PC Security

6.5.1. Desktop PC

(a) Rule

Overall

(a1) The physical security of 'your' client PC is your personal responsibility so please take all reasonable precautions. Be sensible and stay alert to the risks.

(a2) All PCs MUST be assigned to a unique responsible official even if one is used by multiple officials.

(a3) You are personally accountable for all network and systems access under your user ID, so keep your password absolutely secret. The password must be robust and be changed periodically. Never share it with anyone, not even members of your family, friends or IT staff.

(a4) Avoid leaving a PC unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the machine.

Virus Protection

(a5) Viruses are a major threat to NiDA and client PCs are particularly vulnerable if their anti-virus software is not kept up-to-date. The virus definition file MUST be updated at least weekly. The easiest way of doing this is simply to log on to the LAN for the automatic update process to run. If you cannot log on for some reason, contact Information Security Office

for advice on obtaining and installing anti-virus updates.

(a6) Always virus-scan any files downloaded to your computer from any source (FD/CD/DVD, USB hard disks and memory sticks, network files, e-mail attachments or files from the Internet). Virus scans must be set to happen automatically. It is also required to initiate scheduled scans at least weekly.

(a7) Report any information security events (such as virus infections) promptly to Information Security Office in order to minimize the damage.

(a8) Respond immediately to any virus warning message on your computer, or if you suspect a virus (e.g. by unusual file activity) by contacting Information Security Office. Do not forward any files or upload data onto the network if you suspect your PC might be infected.

(a9) Be especially careful to virus-scan your system before you send any files. This includes E-mail attachments and FD/CD/DVDs that you create.

(a10) Connect UPS for all desktop PCs not to lose information.

Disposal
(a11) Execute a physical formatting of storage in a PC not to leave any information readable.

(b) Procedure
For All Officials
Anti-virus Protection
(b1) The following procedure is defined to make sure that all PCs have the updated anti-virus software with a certain frequency.

Step	Description	Owner	Records
b1.1	Instruct the submission of anti-virus software scan log.	ISO	n/a
b1.2	Execute scan.	Official	n/a
b1.3	Print out and submit a scan log.	Official	Anti-virus software scan log
b1.4	File a scan log and keep for the defined period.	IS In-charge	n/a
b1.5	Follow up those who has not executed a scan and submitted a log.	IS In-charge	n/a

Virus Detection Handling
(b2) The following procedure is defined to take actions against virus

detection.

Step	Description	Owner	Records
b2.1	Detect an information security event such as virus detection.	Official	n/a
b2.2	Physically off-line from a network immediately.	Official	n/a
b2.3	Inform ISO immediately when the event happens.	Official	Information Security Event Report
b2.4	Analyze the effects of an event and take an appropriate action.	ISO	n/a
b2.5	Terminate any network/application services if necessary.	ISO	n/a
b2.6	Execute an emergent anti-virus protection procedure if necessary.	ISO	n/a
b2.7	Record an analysis and an action in a report.	ISO	(Updated) Information Security Event Report
b2.8	File a report and keep for the defined period.	IS In-charge	n/a

6.5.2. Laptop/Mobile PC

(a) Rule

Overall

The following rules are for laptop/mobile PC specifically. The laptop/mobile PC is also required to implement the rule and procedures defined in 6.5.1 **Desktop PC**.

(a1) Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag or mobile phone. Be extra careful in public places such as restaurants. It takes thieves just a fraction of a second to steal an unattended laptop.

(a2) If you have to leave the PC temporarily unattended in the office, meeting room or hotel room, even for a short while, use a laptop security cable or similar device to attach it firmly to a desk or similar heavy furniture. These locks are not very secure but deter casual thieves.

(a3) Lock the laptop away out of sight when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel. Never leave a laptop visibly unattended in a vehicle. If absolutely necessary, lock it out of sight in the trunk or glove box but it is generally much safer to take it with you.

(a4) Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. Don't drop it or knock it about! Bubble-wrap packaging may be useful. An ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag.

(a5) Government-owned laptops are provided for official use by authorized employees. Do not loan your laptop or allow it to be used by others such as family and friends.

(a6) Keep a note of the maker, model, serial number and the asset owner label (e.g. NiDA) of your laptop but do not keep this information with the laptop. If it is lost or stolen, notify the Police immediately and inform Information Security Office as soon as practicable (within hours not days, please).

Controls against unauthorized access to laptop/mobile PC data

(a7) Be highly recommended to use approved encryption software on all laptop/mobile PCs, choose a long, strong encryption password/phrase and keep it secure. Contact Information Security Office for further information on laptop encryption. If a laptop/mobile PC is lost or stolen, encryption provides extremely strong protection against unauthorized access to the data.

(a8) Do NOT save confidential information on your laptop/mobile PC instead of encrypting described in the previous clause.

(b) Procedure

For All Officials

Lost/Stolen Properties Event Handling

(b1) If a laptop/mobile PC is lost or stolen, follow the procedure described as a normal information security event.

Step	Description	Owner	Records
b1.1	Detect an information security event such as a property lost or stolen.	Official	n/a
b1.2	Notify the Police.	Official	n/a
b1.3	Inform ISO within an hour after the event happens.	Official	Information Security Event Report
b1.4	Analyze the effects of an event and take an	ISO	(Updated) Information

	appropriate action. Record those in a report.		Security Event Report
b1.5	File a report and keep it for the defined period.	IS In-charge	n/a

6.5.3. Storage Devices (Portable Hard Disk / Memory Stick / Memory Card / Floppy Disk)

(a) Rule

Overall

(a1) Put an appropriate strap on those devices to keep them with you firmly. The recent high-tech storage devices are so small that they are easily dropped off and lost.

Virus Protection

(a2) Do NOT auto-run any storage devices when connecting to your computer.

(a3) Always virus-scan any storage devices when connecting to your computer.

Disposal

(a4) Execute a physical formatting of storage or scrap it physically not to leave any information readable.

(b) Procedure

For All Officials

Lost/Stolen Properties Event Handling

(b1) If any storage devices are lost or stolen, follow the procedure described in **Lost/Stolen Properties Event Handling** in **Laptop/Mobile PC** rule and procedures.

6.5.4. Personal Properties

(a) Rule

(a1) Get a permission of Information Security Manager to bring/take personal client PC related properties into/out of an office.

(b) Procedure

(No procedure is applied for this section.)

6.5.5. Software

(a) Rule

Overall

(a1) Install software explicitly allowed by IS manager.

(a2) Configure software according to IS In-charge instruction.

(a3) Apply patches promptly after IS In-charge instructs.

Unlicensed Software

(a4) Be careful about software licences. Most software, unless it is

specifically identified as “freeware” or “public domain software”, may only be installed and/or used if the appropriate licence fee has been paid. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period. Some software is limited to free use by private individuals whereas commercial use requires a license payment. Individuals and organizations are being prosecuted for infringing software copyright: do not risk bringing yourself and NiDA into disrepute by breaking the law.

Unauthorized Software

(a5) Do not download, install or use unauthorized software programs. Unauthorized software could introduce serious security vulnerabilities into the NiDA networks as well as affecting the working of your PC. Software packages that permit the computer to be ‘remote controlled’ (e.g. PCanywhere) and ‘hacking tools’ (e.g. network sniffers and password crackers) are explicitly forbidden on NiDA equipment properties unless they have been explicitly pre-authorized by management for legitimate business purposes. (e.g. Network Working Group for network auditing operation)

Backups

(a6) You must take your own backups of data on a client PC. The simplest way to do this is to logon and upload a data from the PC to the network on a regular basis – ideally daily but weekly at least. If you are unable to access the network, it is your responsibility to take regular off-line backups to FD/CD/DVD, USB hard disk /memory card/sticks etc. Make sure that off-line backups are encrypted and physically secured. Remember, if a client PC is stolen, lost or damaged, or if it simply malfunctions, it may be impossible to retrieve any of the data from the PC. Off-line backups will save you a lot of heartache and extra work.

(b) Procedure

For Information Security Office

Patch Application Instruction

(b1) The following procedure is defined to instruct apply patches.

Step	Description	Owner	Records
b1.1	Update a standard software setting and the latest patches information list periodically. (The list may contains a general clause such as “Always apply windows update promptly unless it is prohibited explicitly.”)	ISO	(Standard software setting and the latest patches information list)
b1.2	Distribute the list to	IS In-charge	n/a

	Officials and enhance them apply promptly.		
b1.3	Apply patches promptly after IS In-charge instructs.	Official	n/a

Software Setting Patrol Check

(b1) The following procedure is defined to audit software setting internally.

Step	Description	Owner	Records
b1.1	Plan and prepare software setting patrol check such as the date and sampled PCs. Instruct the setting before a patrol check.	ISO	n/a
b1.2	Check software settings one by one. When found a nonconformance, instruct a PC owner fix the setting.	IS In-charge	n/a
b1.3	Submit an Information Security Event Report if found a nonconformance.	Official	Information Security Event Report
b1.4	File a report and keep it for the defined period.	IS In-charge	n/a

6.5.6. <u>E-mail</u>

(a) Rule

(a1) E-mail attachments are now the number one source of computer viruses. Avoid opening any e-mail attachment unless you were expecting to receive it from that person.

(a2) Do not use e-mail:

(a2.1) To send confidential/sensitive information, particularly over the Internet, unless it is first encrypted by an encryption system approved by Information Security;

(a2.2) For private or charity work unconnected with the organization's legitimate business;

(a2.3) In ways that could be interpreted as representing or being official public statements on behalf of the organization, unless you are a spokesperson explicitly authorized by management to make such statements;

(a2.4) To send a message from anyone else's account or in their name (including the use of false 'From:' addresses). If authorized by the manager, a secretary may send e-mail on the manager's behalf but should sign the e-mail in their own name per pro ('for and on behalf of') the manager;

(a2.5) To send any disruptive, offensive, unethical, illegal or otherwise inappropriate matter, including offensive comments about race, gender, color, disability, age, sexual orientation, pornography, terrorism, religious beliefs and practice, political beliefs or national origin, hyperlinks or other references to indecent or patently offensive websites and similar materials, jokes, chain letters, virus warnings and hoaxes, charity requests, viruses or other malicious software;

(a2.6) For any other illegal, unethical or unauthorized purpose.

(a3) Apply your professional discretion when using e-mail, for example abiding by the generally accepted rules of e-mail etiquette.

(a4) Review e-mails carefully before sending, especially formal communications with external parties.

(a5) Do not unnecessarily disclose potentially sensitive information in "out of office" messages.

(a6) Except when specifically authorized by management or where necessary for IT system administration purposes, officials must not intercept, divert, modify, delete, save or disclose e-mails.

(a7) Limited personal use of the corporate e-mail systems is permitted at the discretion of local management provided always that it is incidental and occasional, and does not interfere with business. You should have no expectations of privacy: all e-mails traversing the government systems and networks are subject to automated scanning and may be quarantined and/or reviewed by authorized employees.

(a8) Be reasonable about the number and size of e-mails you send and save. Periodically clear out your mailbox, deleting old e-mails that are no longer required and filing messages that need to be kept under appropriate e-mail folders.

Suspension

(The clause will be activated after the government e-mail service installs the auto-scan function.)

(The clause will be activated after the government e-mail service gets stable.)

(b) Procedure

For All Officials

Normal Information Security Events Handling

(b1) The following procedure is defined to report any information security events promptly.

Step	Description	Owner	Records
b1.1	Detect an information security event such as undesirable/unsavory e-mails are delivered.	Official	n/a
b1.2	Inform ISO within an hour after the event happens.	Official	Information Security Event Report
b1.3	Analyze the effects of an event and take an appropriate action. Record those in a report.	ISO	(Updated) Information Security Event Report
b1.4	File a report and keep it for the defined period.	IS In-charge	n/a

6.5.7. <u>Web Browsing</u>

(a) Rule

Overall

(a1) Do not download an executable file without permission from Information Security Manager.

(a2) Download a file only which has a certification.

(a3) Do not click any links in an undesirable web site or e-mail.

(a4) It is highly recommended not to save cookies, which may cause User ID/password leak.

(a5) Set up a web browser associated to the previous clauses.

Inappropriate Materials

(a6) Be sensible! NiDA will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, pictures, videos or e-mail messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the client PC and steer clear of dubious websites. Information Security Office routinely monitors the network and systems for such materials and track use of the Internet: they will report serious/repeated offenders and any illegal materials

directly to Chief Information Security Officer, and disciplinary processes will be initiated. If you receive inappropriate material by e-mail or other means, delete it immediately. If you accidentally browse to an offensive website, click 'back' or close the window straight away. If you routinely receive a lot of spam, call Information Security Office to check your spam settings.

(b) Procedure

For Information Security Office

Web Browser Setting Patrol Check

(b1) The following procedure is defined to audit web browser setting internally.

Step	Description	Owner	Records
b1.1	Plan and prepare web browser settings patrol check such as the date and sampled PCs. Instruct the setting before a patrol check.	ISO	n/a
b1.2	Check web browser settings one by one. When found a nonconformance, instruct a PC owner fix the setting.	IS In-charge	n/a
b1.3	Submit an Information Security Event Report if found a nonconformance.	Official	Information Security Event Report
b1.4	File a report and keep it for the defined period.	IS In-charge	n/a

6.6. Network and Server Security (To be fully defined in a future)

6.6.1. LAN and Internet

(a) Rule

Suspension

This section will be activated after PAIS is integrated with GAIS and system administration will be operated basically on PAIS. Develop a system administration manual for GAIS/PAIS and CamCERT network respectively which includes the updated network architecture/configuration and detailed operation procedures cooperating with other groups such as Information Security Office.

(b) Procedure

(No procedure is applied for this section.)

6.6.2. Server Common

(a) Rule

Suspension

This section will be activated after PAIS is integrated with GAIS and system administration will be operated basically on PAIS. Develop a system administration manual for GAIS and CamCERT system respectively which includes the updated system architecture/configuration and detailed operation procedures cooperating with other groups such as Information Security Office.

(b) Procedure

(No procedure is applied for this section.)

6.7. Application Software Security (To be defined in a future)

(a) Rule

(This section defines the information security requirements to application software and those to an application software development project.)

7. Information Security Training

7.1. Information Security Training Execution

All officials must get Information Security Training at least once a year. The following procedure is defined to plan and conduct information security training.

	Description	Owner	Records
b1.1	Plan information security training both for the experienced and newly-hired officials	ISO	n/a
b1.2	Conduct a training session.	IS In-charge	n/a
b1.3	Record who took the session and keep it for the defined period.	IS In-charge	Training Record

7.2. Promissory Letter Submission

All officials must once submit Promissory Letter to secure information. It is desirable to sign out at the time of training. The following procedure is defined to submit Promissory Letter.

Step	Description	Owner	Records
b2.1	Distribute promissory letter blank.	ISO	n/a
b2.2	Read through, sign out and submit one.	Official	Promissory Letter
b2.3	File and keep it for the defined period.	IS In-charge	n/a

8. Measurement

The following items will be measured by IS In-charge and reported at ISO at least yearly. The report enables to improve ISMS based on an objective detail.

#	Measurement Name	Definition	Authorized by
1	Training Completion Rate	% of those who has completed training among all NiDA Officials	CISO
2	Information Security Event Mean Time to Process Completion by Event Type	Sum up (Process Completion Time - Event Occurred Time) divided by the number of events by Event Type* (Event Type is defined on an Information Security Event Report blank)	CISO
3	Anti-Virus Scan Execution Rate	% of those who has completed anti-virus scan among all NiDA Officials at the time of an anti-virus protection procedure issue.	CISO
4	Promissory Letter Submission Rate	% of those who has submitted Promissory Letter among all NiDA Officials	CISO
	-End of List-		

9. Breach (To be defined in a future)

(a) Rule

(This section defines the penalty against the information security breaches. It needs internal human resources regulation of government officials.)

10. **Records List**

#	Records Name	Reference	Blank drafted by	Authorized by
1	Training Record	Chapter 7.1 Information Security Training Execution	ISO	CISO
2	Information Security Event Report	(1) Virus Detection Handling Procedure in Chapter 6.5.1 Desktop PC (2) Lost/Stolen Properties Handling Procedure in Chapter 6.5.2 Laptop/Mobile PC (3) Software Setting Patrol Check Procedure in Chapter 6.5.5 Software (4) Normal Information Event Handling Procedure in Chapter 6.5.6 E-mail (5) Web Browser Setting Patrol Check Procedure in Chapter 6.5.7 Web Browser	ISO	CISO

3	Anti-virus Software Scan Log	Anti-virus Protection Procedure in Chapter 6.5.1 Desktop PC	ISO	CISO
4	Promissory Letter	Chapter 7.2 Promissory Letter Submission	ISO	CISO
	-End of List-			

SECTION 6
The Statement of Promise
For Government Information Security

The Statement of Promise
for Government Information Security

I hereby state the promise as follows, in order to keep government information secured as an official of Royal Governement of Cambodia.

- I am always compliant with Government Information Management System Policy, and with rules and procedures defined in Government Information Security Rule Book at the ministry I belong to.

- I am responsible for that
  - It is always considered whether I acquire, process or save confidential information. I do not expose information against any risks of leakage, falsification and inaccessibility;
  - It is assured to lock up an office entrance, a cabinet and a desk drawer before walking away for any moment.
  - An auto-detection function of anti-virus software is activated. I update a virus definition file at least weekly. A storage device of my PC is scanned weekly and any external storage devices (e.g. FD, Memory Card/Stick and HDD) has to be also scanned when to connect to my PC.

- I fully understand the information security risks and the breaches of information security may be led to receive any penalties by authority.

Signature_____
(Title:)

Date _____