Dokumentenlenkung

Titel:	IX-SoA
Version:	1.0
Freigabedatum:	14.07.23
Autor:	sguhl
Verantwortlich:	sguhl
Freigegeben durch:	sguhl
Vertraulichkeitsstufe:	öffentlich
Freigegeben für:	interessierte Parteien
Revisionsintervall:	Jährlich
Nächste Revision:	14.07.24

Zweck	SoA des ISMS der avodaq AG

Dokumentenhistorie

Datum	Version	Beschreibung	Autor
14.07.23	1.0	initiale Version	sguhl

Statement of Applicability (Erklärung zur Anwendbarkeit)

Legende (für ausgewählte Maßnahmen und Gründe für die Auswahl von Maßnahmen):
GA: gesetzliche Anforderungen
VA: vertragliche Anforderungen/Verpflichtungen
GA/BP: Geschäftsanforderungen / Best Practices
RM: Ergebnisse der Risikobeurteilung / Anforderungen aus dem Risikomanagement

ID	Maßnahmen-Nr.	Anwendbarkeit (Ja/Nein)	Beschreibung	Begründung bei Ausschluss	Begründung bei Annahme			
					GA	VA	GA/BP	RM
			Anforderungen der ISO/IEC 27001					
			Normkapitel					
1	4.1	Muss	Verstehen der Organisation und ihres Kontextes				x	
2	4.2	Muss	Verstehen der Anforderungen interessierter Parteien				x	
3	4.3	Muss	Festlegung des Anwendungsbereich des Informationssicherheitsmanagementsystems				x	
4	5.1	Muss	Führung und Verpflichtung				x	
5	5.2	Muss	Politik (Informationssicherheitspolitik)				x	
6	5.3	Muss	Rollen, Verantwortlichkeiten, Befugnisse				x	
7	6.1.1	Muss	Allgemeines zum Umgang mit Risiken und Chancen				x	
8	6.1.2	Muss	Informationssicherheitsrisikobeurteilung				x	
9	6.1.3	Muss	Informationssicherheitsrisikobehandlung				x	
10	6.2	Muss	Informationssicherheitsziele und Planung zu deren Erreichung				x	
11	7.1	Muss	Ressourcen				x	
12	7.2	Muss	Kompetenz				x	
13	7.3	Muss	Bewusstsein				x	
14	7.4	Muss	Kommunikation				x	
15	7.5.1	Muss	Dokumentierte Information				x	
16	7.5.2	Muss	Erstellen und Aktualisieren				x	
17	7.5.3	Muss	Lenkung dokumentierter Information				x	
18	8.1	Muss	Betriebliche Planung und Steuerung				x	
19	8.2	Muss	Informationssicherheitsrisikobeurteilung				x	x
20	8.3	Muss	Informationssicherheitsrisikobehandlung				x	x
21	9.1	Muss	Überwachung, Messung, Analyse und Bewertung					x
22	9.2	Muss	Internes Audit					x
23	9.3	Muss	Managementbewertung					x
24	10.1	Muss	Nichtkonformität und Korrekturmaßnahmen					x
25	10.2	Muss	Fortlaufende Verbesserung				x	x
26			**Annex A**					
27	A.5	/	**Informationssicherheitsrichtlinien**					
28	A.5.1	/	Vorgaben der Leitung zur Informationssicherheit				x	
29	A.5.1.1	Ja	Informationssicherheitsrichtlinien				x	
30	A.5.1.2	Ja	Überprüfung der Informationssicherheitsrichtlinien				x	x
31	A.6	/	**Organisation der Informationssicherheit**					
32	A.6.1	/	Interne Organisation				x	
33	A.6.1.1	Ja	Informationssicherheitsrollen und-verantwortlichkeiten				x	x
34	A.6.1.2	Ja	Aufgabentrennung				x	x
35	A.6.1.3	Ja	Kontakt mit Behörden				x	x
36	A.6.1.4	Ja	Kontakt mit speziellen Interessensgruppen				x	x
37	A.6.1.5	Ja	Informationssicherheit im Projektmanagement				x	
38	A.6.2	ja	Mobilgeräte und Telearbeit				x	
39	A.6.2.1	Ja	Richtlinie zu Mobilgeräten				x	x
40	A.6.2.2	Ja	Telearbeit				x	
41	A.7	/	**Personalsicherheit**					
42	A.7.1	/	Vor der Beschäftigung				x	
43	A.7.1.1	Ja	Sicherheitsüberprüfung		x		x	
44	A.7.1.2	Ja	Beschäftigungs- und Vertragsbedingungen		x		x	
45	A.7.2	/	Während der Beschäftigung					x
46	A.7.2.1	Ja	Verantwortung der Leitung				x	x
47	A.7.2.2	Ja	Informationssicherheitsbewusstsein, -ausbildung und -schulung				x	x
48	A.7.2.3	Ja	Maßregelungsprozess		x		x	
49	A.7.3	/	Beendigung und Wechsel der Beschäftigung					
50	A.7.3.1	Ja	Verantwortlichkeiten bei Beendigung und Änderung der Beschäftigung				x	
51	A.8	/	**Verwaltung der Werte**					
52	A.8.1	/	Verantwortlichkeit für Werte					
53	A.8.1.1	Ja	Inventarisierung der Werte				x	
54	A.8.1.2	Ja	Zuständigkeit für Werte				x	
55	A.8.1.3	Ja	Zulässiger Gebrauch von Werten				x	
56	A.8.1.4	Ja	Rückgabe von Werten				x	
57	A.8.2	/	Informationsklassifizierung					
58	A.8.2.1	Ja	Klassifizierung von Information		x	x	x	
59	A.8.2.2	Ja	Kennzeichnung von Information				x	
60	A.8.2.3	Ja	Handhabung von Werten				x	
61	A.8.3	/	Handhabung von Datenträgern					
62	A.8.3.1	Ja	Handhabung von Wechseldatenträgern				x	
63	A.8.3.2	Ja	Entsorgung von Datenträgern				x	
64	A.8.3.3	Ja	Transport von Datenträgern				x	
65	A.9	/	**Zugangssteuerung**					
66	A.9.1	/	Geschäftsanforderungen an die Zugangssteuerung					
67	A.9.1.1	Ja	Zugangssteuerungsrichtlinie			x	x	
68	A.9.1.2	Ja	Zugang zu Netzwerken und Netzwerkdiensten			x	x	
69	A.9.2	/	Benutzerzugangsverwaltung					
70	A.9.2.1	Ja	Registrierung und Deregistrierung von Benutzern				x	
71	A.9.2.2	Ja	Zuteilung von Benutzerzugängen				x	
72	A.9.2.3	Ja	Verwaltung privilegierter Zugangsrechte				x	
73	A.9.2.4	Ja	Verwaltung geheimer Authentisierungsinformationen von Benutzern				x	
74	A.9.2.5	Ja	Überprüfung von Benutzerzugangsrechten				x	
75	A.9.2.6	Ja	Entzug oder Anpassung von Zugangsrechten				x	
76	A.9.3	/	Benutzerverantwortlichkeiten					
77	A.9.3.1	Ja	Gebrauch geheimer Authentisierungsinformation		x	x	x	
78	A.9.4	/	Zugangssteuerung für Systeme und Anwendungen					
79	A.9.4.1	Ja	Informationszugangsbeschränkung			x	x	
80	A.9.4.2	Ja	Sichere Anmeldeverfahren				x	
81	A.9.4.3	Ja	System zur Verwaltung von Kennwörtern				x	
82	A.9.4.4	Ja	Gebrauch von Hilfsprogrammen mit privilegierten Rechten				x	
83	A.9.4.5	Ja	Zugangssteuerung für Quellcode von Programmen			x	x	
84	A.10	/	**Kryptographie**					
85	A.10.1	/	Kryptographische Maßnahmen					
86	A.10.1.1	Ja	Richtlinie zum Gebrauch von kryptographischen Maßnahmen				x	
87	A.10.1.2	Ja	Schlüsselverwaltung				x	
88	A.11	/	**Physische und umgebungsbezogene Sicherheit**					
89	A.11.1	/	Sicherheitsbereiche					
90	A.11.1.1	Ja	Physischer Sicherheitsperimeter				x	
91	A.11.1.2	Ja	Physische Zutrittssteuerung			x	x	
92	A.11.1.3	Ja	Sichern von Büros, Räumen und Einrichtungen			x	x	
93	A.11.1.4	Ja	Schutz vor externen und umweltbedingten Bedrohungen				x	
94	A.11.1.5	Ja	Arbeiten in Sicherheitsbereichen			x	x	
95	A.11.1.6	Ja	Anlieferungs- und Ladebereiche				x	
96	A.11.2	/	Geräte und Betriebsmittel					
97	A.11.2.1	Ja	Platzierung und Schutz von Geräten und Betriebsmitteln				x	
98	A.11.2.2	Ja	Versorgungseinrichtungen				x	
99	A.11.2.3	Ja	Sicherheit der Verkabelung		x		x	
100	A.11.2.4	Ja	Instandhalten von Geräten und Betriebsmitteln		x		x	
101	A.11.2.5	Ja	Entfernen von Werten				x	
102	A.11.2.6	Ja	Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten				x	
103	A.11.2.7	Ja	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln				x	
104	A.11.2.8	Ja	Unbeaufsichtigte Benutzergeräte			x	x	
105	A.11.2.9	ja	Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren			x	x	
106	A.12	/	**Betriebssicherheit**					
107	A.12.1	/	Betriebsabläufe und -verantwortlichkeiten					
108	A.12.1.1	ja	Dokumentierte Bedienabläufe				x	
109	A.12.1.2	ja	Änderungssteuerung				x	
110	A.12.1.3	ja	Kapazitätssteuerung				x	
111	A12.1.4	Ja	Trennung von Entwicklungs-, Test- und Betriebsumgebungen				x	
112	A.12.2	/	Schutz vor Schadsoftware					
113	A.12.2.1	ja	Maßnahmen gegen Schadsoftware				x	
114	A.12.3	/	Datensicherungen					
115	A.12.3.1	ja	Sicherung von Information		x	x	x	
116	A.12.4	/	Protokollierung und Überwachung					
117	A.12.4.1	ja	Ereignisprotokollierung				x	
118	A.12.4.2	ja	Schutz der Protokolinformation				x	
119	A.12.4.3	ja	Administratoren- und Bedienerprotokolle				x	
120	A.12.4.4	ja	Uhrensynchronisation				x	
121	A.12.5.	/	Steuerung von Software im Betrieb					
122	A.12.5.1	ja	Installation von Software auf Systemen im Betrieb				x	
123	A.12.6	/	Handhabung technischer Schwachstellen					
124	A.12.6.1	ja	Handhabung von technischen Schwachstellen				x	
125	A.12.6.2	ja	Einschränkung von Softwareinstallation				x	
126	A.12.7	/	Audit von Informationssystemen					
127	A.12.7.1	ja	Maßnahmen für Audits von Informationssystemen				x	
128	A.13	/	**Kommunikationssicherheit**					
129	A.13.1	/	Netzwerksicherheitsmanagement					
130	A.13.1.1	ja	Netzwerksteuerungsmaßnahmen				x	
131	A.13.1.2	ja	Sicherheit von Netzwerkdiensten				x	
132	A.13.1.3	ja	Trennung von Netzwerken				x	
133	A.13.2	/	Informationsübertragung					
134	A.13.2.1	ja	Richtlinien und Verfahren zur Informationsübertragung			x	x	
135	A.13.2.2	ja	Vereinbarungen zur Informationsübertragung			x	x	
136	A.13.2.3	ja	Elektronische Nachrichtenübermittlung				x	
137	A.13.2.4	ja	Vertraulichkeits- oder Geheimhaltungsvereinbarungen		x	x	x	
138	A.14	/	**Anschaffung, Entwicklung und Instandhalten von Systemen**					
139	A.14.1	/	Sicherheitsanforderungen an Informationssysteme					
140	A.14.1.1	Ja	Analyse und Spezifikation von Informationssicherheitsanforderungen				x	
141	A.14.1.2	Ja	Sicherung von Anwendungsdiensten in öffentlichen Netzwerken				x	
142	A.14.1.3	Ja	Schutz der Transaktionen bei Anwendungsdiensten				x	
143	A.14.2	/	Sicherheit in Entwicklungs- und Unterstützungsprozessen					
144	A.14.2.1	Ja	Richtlinie für sichere Entwicklung			x	x	
145	A.14.2.2	Ja	Verfahren zur Verwaltung von Systemänderungen				x	
146	A.14.2.3	Ja	Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform				x	
147	A.14.2.4	Ja	Beschränkung von Änderungen an Softwarepaketen				x	
148	A.14.2.5	Ja	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme			x	x	
149	A.14.2.6	Ja	Sichere Entwicklungsumgebung				x	
150	A.14.2.7	Ja	Ausgegliederte Entwicklung		x	x	x	
151	A.14.2.8	Ja	Testen der Systemsicherheit				x	
152	A.14.2.9	Ja	Systemabnahmetest				x	
153	A.14.3	/	Testdaten					
154	A.14.3.1	Ja	Schutz von Testdaten		x		x	
155	A.15	/	**Lieferantenbeziehungen**					
156	A.15.1	/	Informationssicherheit in Lieferantenbeziehungen					
157	A.15.1.1	Ja	Informationssicherheitsrichtlinie für Lieferantenbeziehungen			x	x	
158	A.15.1.2	Ja	Behandlung von Sicherheit in Lieferantenvereinbarungen			x	x	
159	A.15.1.3	Ja	Lieferkette für Informations- und Kommunikationstechnologie				x	
160	A.15.2	/	Steuerung der Dienstleistungserbringung von Lieferanten					
161	A.15.2.1	Ja	Überwachung und Überprüfung von Lieferantendienstleistungen				x	
162	A.15.2.2	Ja	Handhabung der Änderungen von Lieferantendienstleistungen				x	
163	A.16	/	**Handhabung von Informationssicherheitsvorfällen**					
164	A.16.1	/	Handhabung von Informationssicherheitsvorfällen und Verbesserungen					
165	A.16.1.1	Ja	Verantwortlichkeiten und Verfahren				x	
166	A.16.1.2	Ja	Meldung von Informationssicherheitsereignissen			x	x	
167	A.16.1.3	Ja	Meldung von Schwächen in der Informationssicherheit				x	
168	A.16.1.4	Ja	Beurteilung von und Entscheidung über Informationssicherheitsereignisse				x	
169	A.16.1.5	Ja	Reaktion auf Informationssicherheitsvorfälle			x	x	
170	A.16.1.6	Ja	Erkenntnisse aus Informationssicherheitsvorfällen				x	
171	A.16.1.7	Ja	Sammeln von Beweismaterial		x		x	
172	A.17	/	**Informationssicherheitsaspekte beim Business Continuity Management**					
173	A.17.1	/	Aufrechterhaltung der Informationssicherheit					
174	A.17.1.1	Ja	Planung der Aufrechterhaltung der Informationssicherheit				x	
175	A.17.1.2	Ja	Umsetzen der Aufrechterhaltung der Informationssicherheit				x	
176	A.17.1.3	Ja	Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit				x	
177	A.17.2	/	Redundanzen					
178	A.17.2.1	Ja	Verfügbarkeit von informationsverarbeitenden Einrichtungen				x	
179	A.18	/	**Compliance**					
180	A.18.1	/	Einhaltung gesetzlicher und vertraglicher Anforderungen					
181	A.18.1.1	Ja	Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen		x	x	x	
182	A.18.1.2	Ja	Geistige Eigentumsrechte		x	x	x	
183	A.18.1.3	Ja	Schutz von Aufzeichnungen		x	x	x	
184	A.18.1.4	Ja	Privatsphäre und Schutz von personenbezogener Information		x	x		
185	A.18.1.5	Ja	Regelungen bezüglich kryptographischer Maßnahmen		x	x	x	
186	A.18.2	/	Überprüfung der Informationssicherheit					
187	A.18.2.1	Ja	Unabhängige Überprüfung der Informationssicherheit			x	x	
188	A.18.2.2	Ja	Einhaltung von Sicherheitsrichtlinien und-standards			x	x	
189	A.18.2.3	Ja	Überprüfung der Einhaltung von technischen Vorgaben				x	