

# Contents

<b>1</b>	<b>Informationssicherheits-Managementsystem Handbuch</b>	<b>17</b>
<b>2</b>	<b>ISMS-Leitlinie / Informationssicherheits-Policy</b>	<b>18</b>
2.1	1. Zweck . . . . .	18
2.2	2. Geltungsbereich . . . . .	18
2.3	3. Grundsätze (Policy Statements) . . . . .	19
2.4	4. Rollen und Verantwortlichkeiten . . . . .	20
2.5	5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	20
2.6	6. Compliance, Monitoring und Durchsetzung . . . . .	21
2.7	7. Ausnahmen . . . . .	21
2.8	8. Referenzen . . . . .	22
<b>3</b>	<b>ISMS-Geltungsbereich (Scope)</b>	<b>23</b>
3.1	1. Scope-Definition . . . . .	23
3.2	2. Scope-Grenzen und Ausschlüsse . . . . .	24
3.3	3. Schnittstellen . . . . .	25
3.4	4. Scope-Diagramm . . . . .	25
3.5	5. Scope-Änderungen und Review . . . . .	26
3.6	6. Referenzen . . . . .	27
<b>4</b>	<b>Kontext der Organisation und interessierte Parteien</b>	<b>28</b>
4.1	1. Kontext der Organisation . . . . .	28
4.2	2. Interessierte Parteien (Stakeholders) . . . . .	29
4.3	3. Anforderungen an das ISMS . . . . .	30
4.4	4. Auswirkungen auf das ISMS . . . . .	31
4.5	5. Review und Aktualisierung . . . . .	31
4.6	6. Referenzen . . . . .	31
<b>5</b>	<b>ISMS-Governance: Rollen und Verantwortlichkeiten</b>	<b>33</b>
5.1	1. ISMS-Governance-Struktur . . . . .	33
5.2	2. Rollenbeschreibungen . . . . .	34
5.3	3. RACI-Matrix: ISMS-Prozesse . . . . .	36
5.4	4. Eskalationspfade . . . . .	38
5.5	5. Referenzen . . . . .	38
<b>6</b>	<b>Dokumentenlenkung / Dokumentierte Information</b>	<b>40</b>
6.1	1. Zweck und Geltungsbereich . . . . .	40

6.2	2. Ablage und Zugriff . . . . .	40
6.3	3. Dokumentenlebenszyklus . . . . .	41
6.4	4. Versionierung . . . . .	43
6.5	5. Dokumentenregister . . . . .	44
6.6	6. Dokumentklassifizierung . . . . .	44
6.7	7. Externe Dokumente . . . . .	45
6.8	8. Aufbewahrungsfristen . . . . .	45
6.9	9. Referenzen . . . . .	45
<b>7</b>	<b>Risikomanagement – Methodik</b>	<b>47</b>
7.1	1. Ziel und Geltungsbereich . . . . .	47
7.2	2. Risikoobjekte . . . . .	47
7.3	3. Risikomanagement-Methodik . . . . .	48
7.4	4. Quellen für Risikoinformationen . . . . .	51
7.5	5. Outputs des Risikomanagements . . . . .	51
7.6	6. Risikomanagement-Zyklus . . . . .	52
7.7	7. Rollen und Verantwortlichkeiten . . . . .	52
7.8	8. Referenzen . . . . .	53
<b>8</b>	<b>Risikokriterien und Risikoakzeptanz</b>	<b>54</b>
8.1	1. Risikoappetit und Toleranz . . . . .	54
8.2	2. Bewertungsdimensionen . . . . .	55
8.3	3. Akzeptanzprozess . . . . .	55
8.4	4. Referenzen . . . . .	56
<b>9</b>	<b>Risikoregister (Template)</b>	<b>57</b>
9.1	1. Zweck und Anleitung . . . . .	57
9.2	2. Risikoregister-Tabelle . . . . .	58
9.3	3. Risikokategorien und Klassifizierung . . . . .	59
9.4	4. Risikobewertung . . . . .	60
9.5	5. Risiko-Eigentümer und Verantwortlichkeiten . . . . .	61
9.6	6. Risiko-Reporting . . . . .	61
9.7	7. Risiko-Review und Aktualisierung . . . . .	62
9.8	8. Verknüpfungen und Referenzen . . . . .	62
9.9	Änderungshistorie . . . . .	62
<b>10</b>	<b>Risikobehandlungsplan (RTP) – Template</b>	<b>64</b>
10.1	1. Ziel und Geltungsbereich . . . . .	64
10.2	2. Risikobehandlungsplan-Tabelle . . . . .	65
10.3	3. Maßnahmenpriorisierung . . . . .	66
10.4	4. Maßnahmendetails . . . . .	67
10.5	5. Control-Mapping (Annex A) . . . . .	67
10.6	6. Ressourcenplanung und Budgetierung . . . . .	68
10.7	7. Abhängigkeiten und Risiken der Umsetzung . . . . .	69
10.8	8. Tracking und Reporting . . . . .	70
10.9	9. Wirksamkeitsprüfung . . . . .	70
10.10	10. Rollen und Verantwortlichkeiten . . . . .	70
10.11	11. Referenzen . . . . .	71

10.12 Änderungshistorie . . . . .	71
<b>11 Statement of Applicability (SoA) – Template</b>	<b>73</b>
11.1 1. Zweck und Geltungsbereich . . . . .	73
11.2 2. Control-Auswahlkriterien . . . . .	74
11.3 3. Statement of Applicability (SoA) - Übersicht . . . . .	74
11.4 4. SoA-Tabelle: Organisational Controls (5.x) . . . . .	75
11.5 5. SoA-Tabelle: People Controls (6.x) . . . . .	76
11.6 6. SoA-Tabelle: Physical Controls (7.x) . . . . .	78
11.7 7. SoA-Tabelle: Technological Controls (8.x) . . . . .	80
11.8 8. Nicht anwendbare Controls . . . . .	80
11.9 9. Verknüpfungen und Referenzen . . . . .	81
11.10 10. Review und Aktualisierung . . . . .	81
11.11 11. Referenzen . . . . .	81
11.12 Änderungshistorie . . . . .	82
<b>12 Informationssicherheitsziele und Metriken</b>	<b>83</b>
12.1 1. Informationssicherheitsziele . . . . .	83
12.2 2. Key Performance Indicators (KPIs) . . . . .	84
12.3 3. Messmethoden und Datenquellen . . . . .	85
12.4 4. Maßnahmen zur Zielerreichung . . . . .	86
12.5 5. Review und Anpassung . . . . .	86
12.6 6. Referenzen . . . . .	86
<b>13 Schulung, Awareness und Kompetenz</b>	<b>88</b>
13.1 1. Zweck und Ziele . . . . .	88
13.2 2. Zielgruppen . . . . .	88
13.3 3. Schulungsplan . . . . .	89
13.4 4. Awareness-Kampagnen . . . . .	91
13.5 5. Phishing-Simulationen . . . . .	91
13.6 6. Wirksamkeitsprüfung . . . . .	92
13.7 7. Schulungsnachweise . . . . .	92
13.8 8. Rollen und Verantwortlichkeiten . . . . .	92
13.9 9. Budget und Ressourcen . . . . .	93
13.10 10. Referenzen . . . . .	93
<b>14 Internes Auditprogramm (Template)</b>	<b>95</b>
14.1 1. Zweck und Geltungsbereich . . . . .	95
14.2 2. Audit-Ansatz . . . . .	95
14.3 3. Jahresplan . . . . .	96
14.4 4. Audit-Prozess . . . . .	97
14.5 5. Audit-Findings . . . . .	98
14.6 6. Audit-Bericht . . . . .	99
14.7 7. Auditor-Qualifikation . . . . .	99
14.8 8. Audit-Metriken . . . . .	100
14.9 9. Rollen und Verantwortlichkeiten . . . . .	100
14.10 10. Referenzen . . . . .	101
<b>15 Management Review (Template)</b>	<b>102</b>

15.1 1. Management Review-Übersicht . . . . .	102
15.2 2. Inputs (Clause 9.3.2) . . . . .	103
15.3 3. Outputs / Entscheidungen (Clause 9.3.3) . . . . .	106
15.4 4. Zusammenfassung und Bewertung . . . . .	107
15.5 5. Anhänge . . . . .	108
15.6 6. Referenzen . . . . .	108
15.7 Änderungshistorie . . . . .	108
<b>16 Nichtkonformitäten und Korrekturmaßnahmen</b>	<b>110</b>
16.1 1. Zweck und Ziel . . . . .	110
16.2 2. Prozess . . . . .	111
16.3 3. Nichtkonformitäten-Register . . . . .	113
16.4 4. Priorisierung und Fristen . . . . .	113
16.5 5. Ursachenanalyse-Methoden . . . . .	114
16.6 6. Wirksamkeitsprüfung . . . . .	114
16.7 7. Lessons Learned . . . . .	115
16.8 8. Rollen und Verantwortlichkeiten . . . . .	115
16.9 9. Metriken und Reporting . . . . .	115
16.10 10. Referenzen . . . . .	116
<b>17 Kontinuierliche Verbesserung (KVP) im ISMS</b>	<b>117</b>
17.1 1. Zweck und Ziele . . . . .	117
17.2 2. Quellen für Verbesserungen . . . . .	118
17.3 3. KVP-Backlog . . . . .	119
17.4 4. Verbesserungsprozess . . . . .	121
17.5 5. Verbesserungskategorien . . . . .	121
17.6 6. Lessons Learned . . . . .	122
17.7 7. Innovation und Best Practices . . . . .	123
17.8 8. Metriken und Reporting . . . . .	123
17.9 9. Rollen und Verantwortlichkeiten . . . . .	123
17.10 10. Referenzen . . . . .	124
<b>18 Policy: Akzeptable Nutzung IT</b>	<b>125</b>
18.1 1. Zweck . . . . .	125
18.2 2. Geltungsbereich . . . . .	125
18.3 3. Grundsätze (Policy Statements) . . . . .	126
18.4 4. Rollen und Verantwortlichkeiten . . . . .	126
18.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	127
18.6 6. Compliance, Monitoring und Durchsetzung . . . . .	127
18.7 7. Ausnahmen . . . . .	128
18.8 8. Referenzen . . . . .	128
<b>19 Richtlinie: Akzeptable Nutzung IT</b>	<b>129</b>
19.1 1. Zweck und Geltungsbereich . . . . .	129
19.2 2. Detaillierte Nutzungsregeln . . . . .	129
19.3 3. Monitoring und Überwachung . . . . .	132
19.4 4. Schulung und Awareness . . . . .	132
19.5 5. Ausnahmen und Sonderfälle . . . . .	133

19.6 6. Technische Implementierung . . . . .	133
19.7 7. Compliance und Audit . . . . .	134
19.8 8. Review und Aktualisierung . . . . .	134
19.9 9. Referenzen . . . . .	134
<b>20 Policy: Zugriffssteuerung und Identitätsmanagement</b>	<b>136</b>
20.1 1. Zweck . . . . .	136
20.2 2. Geltungsbereich . . . . .	136
20.3 3. Grundsätze (Policy Statements) . . . . .	137
20.4 4. Rollen und Verantwortlichkeiten . . . . .	137
20.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	138
20.6 6. Compliance, Monitoring und Durchsetzung . . . . .	139
20.7 7. Ausnahmen . . . . .	139
20.8 8. Referenzen . . . . .	139
<b>21 Richtlinie: IAM - Joiner, Mover, Leaver und Zugriffsanträge</b>	<b>141</b>
21.1 1. Zweck und Geltungsbereich . . . . .	141
21.2 2. Joiner-Prozess (Onboarding) . . . . .	141
21.3 3. Mover-Prozess (Rollenwechsel) . . . . .	143
21.4 4. Leaver-Prozess (Offboarding) . . . . .	143
21.5 5. Zugriffsanträge (Access Requests) . . . . .	144
21.6 6. Rezertifizierung . . . . .	145
21.7 7. Technische Implementierung . . . . .	145
21.8 8. Compliance und Audit . . . . .	146
21.9 9. Referenzen . . . . .	146
<b>22 Policy: Authentisierung und Passwörter</b>	<b>148</b>
22.1 1. Zweck . . . . .	148
22.2 2. Geltungsbereich . . . . .	148
22.3 3. Grundsätze (Policy Statements) . . . . .	149
22.4 4. Rollen und Verantwortlichkeiten . . . . .	150
22.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	150
22.6 6. Compliance, Monitoring und Durchsetzung . . . . .	151
22.7 7. Ausnahmen . . . . .	151
22.8 8. Referenzen . . . . .	151
<b>23 Richtlinie: MFA, Passwortregeln und Session Management</b>	<b>153</b>
23.1 1. Zweck und Geltungsbereich . . . . .	153
23.2 2. Multi-Faktor-Authentifizierung (MFA) . . . . .	153
23.3 3. Passwortrichtlinien . . . . .	155
23.4 4. Session Management . . . . .	156
23.5 5. Authentifizierungsmethoden . . . . .	156
23.6 6. Service-Accounts und technische Accounts . . . . .	157
23.7 7. Monitoring und Alerting . . . . .	157
23.8 8. Compliance und Audit . . . . .	158
23.9 9. Referenzen . . . . .	158
<b>24 Policy: Kryptografie und Schlüsselmanagement</b>	<b>160</b>
24.1 1. Zweck . . . . .	160

24.2 2. Geltungsbereich . . . . .	160
24.3 3. Grundsätze (Policy Statements) . . . . .	161
24.4 4. Rollen und Verantwortlichkeiten . . . . .	162
24.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	162
24.6 6. Compliance, Monitoring und Durchsetzung . . . . .	163
24.7 7. Ausnahmen . . . . .	163
24.8 8. Referenzen . . . . .	164
<b>25 Richtlinie: Key Management und Verschlüsselung</b>	<b>165</b>
25.1 1. Zweck und Geltungsbereich . . . . .	165
25.2 2. Kryptographische Standards . . . . .	165
25.3 3. Schlüsselmanagement . . . . .	166
25.4 4. Zertifikatsmanagement . . . . .	167
25.5 5. Verschlüsselung von Daten . . . . .	168
25.6 6. E-Mail-Verschlüsselung . . . . .	169
25.7 7. Backup-Verschlüsselung . . . . .	169
25.8 8. Cloud-Verschlüsselung . . . . .	169
25.9 9. Compliance und Audit . . . . .	170
25.10 10. Referenzen . . . . .	170
<b>26 Policy: Datenklassifizierung und Informationshandling</b>	<b>171</b>
26.1 1. Zweck . . . . .	171
26.2 2. Geltungsbereich . . . . .	171
26.3 3. Grundsätze (Policy Statements) . . . . .	172
26.4 4. Rollen und Verantwortlichkeiten . . . . .	173
26.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	173
26.6 6. Compliance, Monitoring und Durchsetzung . . . . .	174
26.7 7. Ausnahmen . . . . .	174
26.8 8. Referenzen . . . . .	175
<b>27 Richtlinie: Datenklassifizierung, Labeling und Handling</b>	<b>176</b>
27.1 1. Zweck und Geltungsbereich . . . . .	176
27.2 2. Klassifizierungsstufen . . . . .	176
27.3 3. Klassifizierungsprozess . . . . .	177
27.4 4. Labeling-Verfahren . . . . .	178
27.5 5. Handling-Anforderungen . . . . .	178
27.6 6. Data Loss Prevention (DLP) . . . . .	179
27.7 7. Schulung und Awareness . . . . .	179
27.8 8. Compliance und Audit . . . . .	180
27.9 9. Referenzen . . . . .	180
<b>28 Policy: Asset Management</b>	<b>181</b>
28.1 1. Zweck . . . . .	181
28.2 2. Geltungsbereich . . . . .	181
28.3 3. Grundsätze (Policy Statements) . . . . .	182
28.4 4. Rollen und Verantwortlichkeiten . . . . .	183
28.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	183
28.6 6. Compliance, Monitoring und Durchsetzung . . . . .	184

28.7 7. Ausnahmen . . . . .	184
28.8 8. Referenzen . . . . .	185
<b>29 Richtlinie: Asset Inventory, Tagging und Entsorgung</b>	<b>186</b>
29.1 1. Zweck und Geltungsbereich . . . . .	186
29.2 2. Asset-Kategorien . . . . .	186
29.3 3. Asset-Inventarisierung . . . . .	187
29.4 4. Asset-Tagging . . . . .	188
29.5 5. Asset-Lifecycle-Management . . . . .	188
29.6 6. Sichere Datenvernichtung . . . . .	189
29.7 7. Asset-Entsorgung . . . . .	189
29.8 8. Compliance und Audit . . . . .	190
29.9 9. Referenzen . . . . .	190
<b>30 Policy: Logging und Monitoring</b>	<b>192</b>
30.1 1. Zweck . . . . .	192
30.2 2. Geltungsbereich . . . . .	192
30.3 3. Grundsätze (Policy Statements) . . . . .	193
30.4 4. Rollen und Verantwortlichkeiten . . . . .	194
30.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	194
30.6 6. Compliance, Monitoring und Durchsetzung . . . . .	195
30.7 7. Ausnahmen . . . . .	195
30.8 8. Referenzen . . . . .	196
<b>31 Richtlinie: Logging, SIEM und Audit Trails</b>	<b>197</b>
31.1 1. Zweck und Geltungsbereich . . . . .	197
31.2 2. Logging-Anforderungen . . . . .	197
31.3 3. SIEM-Integration . . . . .	198
31.4 4. Audit Trails . . . . .	199
31.5 5. Log-Retention . . . . .	200
31.6 6. Log-Sicherheit . . . . .	200
31.7 7. Monitoring und Alerting . . . . .	201
31.8 8. Compliance und Audit . . . . .	201
31.9 9. Referenzen . . . . .	201
<b>32 Policy: Vulnerability und Patch Management</b>	<b>203</b>
32.1 1. Zweck . . . . .	203
32.2 2. Geltungsbereich . . . . .	203
32.3 3. Grundsätze (Policy Statements) . . . . .	204
32.4 4. Rollen und Verantwortlichkeiten . . . . .	204
32.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	205
32.6 6. Compliance, Monitoring und Durchsetzung . . . . .	206
32.7 7. Ausnahmen . . . . .	206
32.8 8. Referenzen . . . . .	206
<b>33 Richtlinie: Vulnerability Scans, Patching und Exploitation Response</b>	<b>208</b>
33.1 1. Zweck und Geltungsbereich . . . . .	208
33.2 2. Vulnerability Scanning . . . . .	208
33.3 3. Schwachstellen-Bewertung . . . . .	209

33.4 4. Patch Management . . . . .	210
33.5 5. Exploitation Response . . . . .	210
33.6 6. Vulnerability Disclosure . . . . .	211
33.7 7. Compliance und Audit . . . . .	211
33.8 8. Referenzen . . . . .	212
<b>34 Policy: Change und Release Management</b>	<b>213</b>
34.1 1. Zweck . . . . .	213
34.2 2. Geltungsbereich . . . . .	213
34.3 3. Grundsätze (Policy Statements) . . . . .	214
34.4 4. Rollen und Verantwortlichkeiten . . . . .	214
34.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	215
34.6 6. Compliance, Monitoring und Durchsetzung . . . . .	216
34.7 7. Ausnahmen . . . . .	216
34.8 8. Referenzen . . . . .	216
<b>35 Richtlinie: Change Management mit Sicherheitsfreigaben</b>	<b>218</b>
35.1 1. Zweck und Geltungsbereich . . . . .	218
35.2 2. Change-Kategorien . . . . .	218
35.3 3. Change-Management-Prozess . . . . .	219
35.4 4. Emergency Changes . . . . .	220
35.5 5. Sicherheitskontrollen . . . . .	220
35.6 6. Testing und Validation . . . . .	221
35.7 7. Dokumentation und Audit . . . . .	221
35.8 8. Referenzen . . . . .	222
<b>36 Policy: Secure Development</b>	<b>223</b>
36.1 1. Zweck . . . . .	223
36.2 2. Geltungsbereich . . . . .	223
36.3 3. Grundsätze (Policy Statements) . . . . .	224
36.4 4. Rollen und Verantwortlichkeiten . . . . .	224
36.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	225
36.6 6. Compliance, Monitoring und Durchsetzung . . . . .	226
36.7 7. Ausnahmen . . . . .	226
36.8 8. Referenzen . . . . .	226
<b>37 Richtlinie: Secure SDLC, Code Reviews und Secrets Management</b>	<b>228</b>
37.1 1. Zweck und Geltungsbereich . . . . .	228
37.2 2. Secure SDLC Phasen . . . . .	228
37.3 3. Secure Coding Standards . . . . .	229
37.4 4. Code Reviews . . . . .	230
37.5 5. Secrets Management . . . . .	230
37.6 6. Dependency Management . . . . .	231
37.7 7. CI/CD Security . . . . .	231
37.8 8. Security Testing . . . . .	232
37.9 9. Compliance und Audit . . . . .	232
37.10 10. Referenzen . . . . .	232
<b>38 Policy: Incident Management</b>	<b>234</b>

38.1 1. Zweck . . . . .	234
38.2 2. Geltungsbereich . . . . .	234
38.3 3. Grundsätze (Policy Statements) . . . . .	235
38.4 4. Rollen und Verantwortlichkeiten . . . . .	235
38.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	236
38.6 6. Compliance, Monitoring und Durchsetzung . . . . .	237
38.7 7. Ausnahmen . . . . .	237
38.8 8. Referenzen . . . . .	238
<b>39 Richtlinie: Incident Response und Major Incident Prozess</b>	<b>239</b>
39.1 1. Zweck und Geltungsbereich . . . . .	239
39.2 2. Incident-Kategorien . . . . .	239
39.3 3. Incident-Response-Prozess . . . . .	240
39.4 4. Major Incident Management . . . . .	241
39.5 5. Security Incident Response . . . . .	242
39.6 6. Incident-Kommunikation . . . . .	242
39.7 7. Compliance und Audit . . . . .	243
39.8 8. Referenzen . . . . .	243
<b>40 Policy: Backup und Wiederherstellung</b>	<b>244</b>
40.1 1. Zweck . . . . .	244
40.2 2. Geltungsbereich . . . . .	244
40.3 3. Grundsätze (Policy Statements) . . . . .	245
40.4 4. Rollen und Verantwortlichkeiten . . . . .	245
40.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	246
40.6 6. Compliance, Monitoring und Durchsetzung . . . . .	247
40.7 7. Ausnahmen . . . . .	247
40.8 8. Referenzen . . . . .	247
<b>41 Richtlinie: Backup, Restore und Regelmäßige Tests</b>	<b>249</b>
41.1 1. Zweck und Geltungsbereich . . . . .	249
41.2 2. Backup-Strategie . . . . .	249
41.3 3. Backup-Implementierung . . . . .	250
41.4 4. Restore-Prozesse . . . . .	251
41.5 5. Backup-Monitoring . . . . .	251
41.6 6. Backup-Tests . . . . .	252
41.7 7. Backup-Sicherheit . . . . .	252
41.8 8. Compliance und Audit . . . . .	253
41.9 9. Referenzen . . . . .	253
<b>42 Policy: Business Continuity ICT Readiness</b>	<b>254</b>
42.1 1. Zweck . . . . .	254
42.2 2. Geltungsbereich . . . . .	254
42.3 3. Grundsätze (Policy Statements) . . . . .	255
42.4 4. Rollen und Verantwortlichkeiten . . . . .	255
42.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	256
42.6 6. Compliance, Monitoring und Durchsetzung . . . . .	257
42.7 7. Ausnahmen . . . . .	257

42.8 8. Referenzen . . . . .	257
<b>43 Richtlinie: ICT Disaster Recovery - Schnittstellen zu BCM</b>	<b>259</b>
43.1 1. Zweck und Geltungsbereich . . . . .	259
43.2 2. ICT Disaster Recovery Strategie . . . . .	259
43.3 3. DR-Infrastruktur . . . . .	260
43.4 4. Schnittstellen zu BCM . . . . .	260
43.5 5. DR-Aktivierung . . . . .	261
43.6 6. DR-Tests . . . . .	261
43.7 7. Compliance und Audit . . . . .	261
43.8 8. Referenzen . . . . .	262
<b>44 Policy: Lieferanten und Cloud Sicherheit</b>	<b>263</b>
44.1 1. Zweck . . . . .	263
44.2 2. Geltungsbereich . . . . .	263
44.3 3. Grundsätze (Policy Statements) . . . . .	264
44.4 4. Rollen und Verantwortlichkeiten . . . . .	264
44.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	265
44.6 6. Compliance, Monitoring und Durchsetzung . . . . .	266
44.7 7. Ausnahmen . . . . .	266
44.8 8. Referenzen . . . . .	266
<b>45 Richtlinie: Third-Party Risk Assessment und Cloud Controls</b>	<b>268</b>
45.1 1. Zweck und Geltungsbereich . . . . .	268
45.2 2. Third-Party Risk Assessment . . . . .	268
45.3 3. Cloud Security Controls . . . . .	269
45.4 4. Vertragsmanagement . . . . .	270
45.5 5. Lieferanten-Risikomanagement . . . . .	270
45.6 6. Compliance und Audit . . . . .	270
45.7 7. Referenzen . . . . .	271
<b>46 Policy: Physische Sicherheit</b>	<b>272</b>
46.1 1. Zweck . . . . .	272
46.2 2. Geltungsbereich . . . . .	272
46.3 3. Grundsätze (Policy Statements) . . . . .	273
46.4 4. Rollen und Verantwortlichkeiten . . . . .	273
46.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	274
46.6 6. Compliance, Monitoring und Durchsetzung . . . . .	275
46.7 7. Ausnahmen . . . . .	275
46.8 8. Referenzen . . . . .	275
<b>47 Richtlinie: Zutritt, Besucher und Schutz von Equipment</b>	<b>277</b>
47.1 1. Zweck und Geltungsbereich . . . . .	277
47.2 2. Sicherheitszonen . . . . .	277
47.3 3. Zutrittskontrollsysteem . . . . .	278
47.4 4. Besuchermanagement . . . . .	278
47.5 5. Physischer Schutz von Equipment . . . . .	279
47.6 6. Videoüberwachung . . . . .	279
47.7 7. Notfallzugang . . . . .	279

47.8 8. Compliance und Audit . . . . .	280
47.9 9. Referenzen . . . . .	280
<b>48 Policy: Mobile Device und Remote Work</b>	<b>281</b>
48.1 1. Zweck . . . . .	281
48.2 2. Geltungsbereich . . . . .	281
48.3 3. Grundsätze (Policy Statements) . . . . .	282
48.4 4. Rollen und Verantwortlichkeiten . . . . .	282
48.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	283
48.6 6. Compliance, Monitoring und Durchsetzung . . . . .	284
48.7 7. Ausnahmen . . . . .	284
48.8 8. Referenzen . . . . .	284
<b>49 Richtlinie: MDM, Bring Your Own Device und Remote Access</b>	<b>286</b>
49.1 1. Zweck und Geltungsbereich . . . . .	286
49.2 2. Mobile Device Management (MDM) . . . . .	286
49.3 3. BYOD (Bring Your Own Device) . . . . .	287
49.4 4. Remote Access . . . . .	288
49.5 5. Remote Work Security . . . . .	288
49.6 6. Mobile Application Management (MAM) . . . . .	289
49.7 7. Incident Response . . . . .	289
49.8 8. Compliance und Audit . . . . .	289
49.9 9. Referenzen . . . . .	289
<b>50 Policy: HR Security</b>	<b>291</b>
50.1 1. Zweck . . . . .	291
50.2 2. Geltungsbereich . . . . .	291
50.3 3. Grundsätze (Policy Statements) . . . . .	292
50.4 4. Rollen und Verantwortlichkeiten . . . . .	292
50.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	293
50.6 6. Compliance, Monitoring und Durchsetzung . . . . .	294
50.7 7. Ausnahmen . . . . .	294
50.8 8. Referenzen . . . . .	294
<b>51 Richtlinie: HR Security - Onboarding, Rollenwechsel, Offboarding</b>	<b>296</b>
51.1 1. Zweck und Geltungsbereich . . . . .	296
51.2 2. Pre-Employment . . . . .	296
51.3 3. Onboarding . . . . .	297
51.4 4. Rollenwechsel (Mover) . . . . .	297
51.5 5. Offboarding . . . . .	298
51.6 6. Vertraulichkeitsverpflichtungen . . . . .	298
51.7 7. Disziplinarmaßnahmen . . . . .	298
51.8 8. Externe Auftragnehmer . . . . .	299
51.9 9. Compliance und Audit . . . . .	299
51.10 10. Referenzen . . . . .	300
<b>52 Policy: Konfiguration und Hardening</b>	<b>301</b>
52.1 1. Zweck . . . . .	301
52.2 2. Geltungsbereich . . . . .	301

52.3 3. Grundsätze (Policy Statements) . . . . .	302
52.4 4. Rollen und Verantwortlichkeiten . . . . .	302
52.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	303
52.6 6. Compliance, Monitoring und Durchsetzung . . . . .	304
52.7 7. Ausnahmen . . . . .	304
52.8 8. Referenzen . . . . .	304
<b>53 Richtlinie: Sicherheitsbaselines, Hardening und Konfigurationsänderungen</b>	<b>306</b>
53.1 1. Zweck und Geltungsbereich . . . . .	306
53.2 2. Sicherheitsbaselines . . . . .	306
53.3 3. Hardening-Prozess . . . . .	307
53.4 4. Configuration Management . . . . .	308
53.5 5. Konfigurationsänderungen . . . . .	308
53.6 6. Ausnahmen und Abweichungen . . . . .	308
53.7 7. Compliance-Monitoring . . . . .	309
53.8 8. Hardening-Standards . . . . .	309
53.9 9. Compliance und Audit . . . . .	310
53.10 10. Referenzen . . . . .	310
<b>54 Policy: Datenschutz Schnittstellen</b>	<b>311</b>
54.1 1. Zweck . . . . .	311
54.2 2. Geltungsbereich . . . . .	311
54.3 3. Grundsätze (Policy Statements) . . . . .	312
54.4 4. Rollen und Verantwortlichkeiten . . . . .	312
54.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	313
54.6 6. Compliance, Monitoring und Durchsetzung . . . . .	314
54.7 7. Ausnahmen . . . . .	314
54.8 8. Referenzen . . . . .	314
<b>55 Richtlinie: Datenschutz-Anforderungen und Datenverarbeitung</b>	<b>316</b>
55.1 1. Zweck und Geltungsbereich . . . . .	316
55.2 2. DSGVO-Grundprinzipien . . . . .	316
55.3 3. Verzeichnis von Verarbeitungstätigkeiten (VVT) . . . . .	317
55.4 4. Datenschutz-Folgenabschätzung (DSFA) . . . . .	317
55.5 5. Betroffenenrechte . . . . .	318
55.6 6. Auftragsverarbeitung . . . . .	319
55.7 7. Datenschutzverletzungen (Data Breaches) . . . . .	319
55.8 8. Internationale Datentransfers . . . . .	319
55.9 9. Compliance und Audit . . . . .	320
55.10 10. Referenzen . . . . .	320
<b>56 Policy: Aufbewahrung und Löschung</b>	<b>321</b>
56.1 1. Zweck . . . . .	321
56.2 2. Geltungsbereich . . . . .	321
56.3 3. Grundsätze (Policy Statements) . . . . .	322
56.4 4. Rollen und Verantwortlichkeiten . . . . .	322
56.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	323
56.6 6. Compliance, Monitoring und Durchsetzung . . . . .	324

56.7 7. Ausnahmen . . . . .	324
56.8 8. Referenzen . . . . .	324
<b>57 Richtlinie: Records Retention und Sichere Löschung</b>	<b>326</b>
57.1 1. Zweck und Geltungsbereich . . . . .	326
57.2 2. Aufbewahrungsfristen . . . . .	326
57.3 3. Retention-Management . . . . .	327
57.4 4. Sichere Löschung . . . . .	328
57.5 5. E-Mail-Archivierung . . . . .	328
57.6 6. Datenminimierung . . . . .	329
57.7 7. Cloud-Daten-Lösung . . . . .	329
57.8 8. Compliance und Audit . . . . .	329
57.9 9. Referenzen . . . . .	330
<b>58 Policy: Netzwerksicherheit</b>	<b>331</b>
58.1 1. Zweck . . . . .	331
58.2 2. Geltungsbereich . . . . .	331
58.3 3. Grundsätze (Policy Statements) . . . . .	332
58.4 4. Rollen und Verantwortlichkeiten . . . . .	332
58.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	333
58.6 6. Compliance, Monitoring und Durchsetzung . . . . .	334
58.7 7. Ausnahmen . . . . .	334
58.8 8. Referenzen . . . . .	335
<b>59 Richtlinie: Segmentierung, Firewalling und Network Access Control</b>	<b>336</b>
59.1 1. Zweck und Geltungsbereich . . . . .	336
59.2 2. Netzwerk-Segmentierung . . . . .	336
59.3 3. Firewall-Management . . . . .	337
59.4 4. Network Access Control (NAC) . . . . .	338
59.5 5. Intrusion Detection/Prevention (IDS/IPS) . . . . .	338
59.6 6. VPN und Remote Access . . . . .	339
59.7 7. Wireless Security . . . . .	339
59.8 8. Network Monitoring . . . . .	339
59.9 9. Compliance und Audit . . . . .	340
59.10 10. Referenzen . . . . .	340
<b>60 Policy: Endpoint Security</b>	<b>341</b>
60.1 1. Zweck . . . . .	341
60.2 2. Geltungsbereich . . . . .	341
60.3 3. Grundsätze (Policy Statements) . . . . .	342
60.4 4. Rollen und Verantwortlichkeiten . . . . .	343
60.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	343
60.6 6. Compliance, Monitoring und Durchsetzung . . . . .	344
60.7 7. Ausnahmen . . . . .	344
60.8 8. Referenzen . . . . .	345
<b>61 Richtlinie: EDR, Antivirus, Host-Firewall und Device Compliance</b>	<b>346</b>
61.1 1. Zweck und Geltungsbereich . . . . .	346
61.2 2. Endpoint Detection and Response (EDR) . . . . .	346

61.3 3. Antivirus (AV) . . . . .	347
61.4 4. Host-Firewall . . . . .	348
61.5 5. Device Compliance . . . . .	348
61.6 6. Patch Management . . . . .	349
61.7 7. Application Control . . . . .	349
61.8 8. USB und Removable Media . . . . .	349
61.9 9. Monitoring und Alerting . . . . .	350
61.10 10. Compliance und Audit . . . . .	350
61.11 11. Referenzen . . . . .	350
<b>62 Policy: Ausnahmen und Risk Waivers</b>	<b>352</b>
62.1 1. Zweck . . . . .	352
62.2 2. Geltungsbereich . . . . .	352
62.3 3. Grundsätze (Policy Statements) . . . . .	353
62.4 4. Rollen und Verantwortlichkeiten . . . . .	354
62.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	354
62.6 6. Compliance, Monitoring und Durchsetzung . . . . .	355
62.7 7. Ausnahmen . . . . .	355
62.8 8. Referenzen . . . . .	355
<b>63 Richtlinie: Ausnahmenprozess</b>	<b>357</b>
63.1 1. Zweck und Geltungsbereich . . . . .	357
63.2 2. Ausnahmen-Kategorien . . . . .	357
63.3 3. Ausnahmenprozess . . . . .	358
63.4 4. Monitoring und Review . . . . .	359
63.5 5. Beendigung von Ausnahmen . . . . .	359
63.6 6. Reporting . . . . .	360
63.7 7. Compliance und Audit . . . . .	360
63.8 8. Beispiele . . . . .	360
63.9 9. Referenzen . . . . .	361
<b>64 Policy: Informationsübertragung und Kommunikation</b>	<b>362</b>
64.1 1. Zweck . . . . .	362
64.2 2. Geltungsbereich . . . . .	362
64.3 3. Grundsätze (Policy Statements) . . . . .	363
64.4 4. Rollen und Verantwortlichkeiten . . . . .	364
64.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	364
64.6 6. Compliance, Monitoring und Durchsetzung . . . . .	365
64.7 7. Ausnahmen . . . . .	365
64.8 8. Referenzen . . . . .	366
<b>65 Richtlinie: E-Mail, Sharing und Zusammenarbeitstools</b>	<b>367</b>
65.1 1. Zweck und Geltungsbereich . . . . .	367
65.2 2. E-Mail-Sicherheit . . . . .	367
65.3 3. File-Sharing . . . . .	368
65.4 4. Collaboration-Tools . . . . .	369
65.5 5. Externe Kommunikation . . . . .	369
65.6 6. Mobile Kommunikation . . . . .	370

65.7 7. Data Loss Prevention (DLP) . . . . .	370
65.8 8. Compliance und Audit . . . . .	370
65.9 9. Referenzen . . . . .	371
<b>66 Policy: Security in Projects</b>	<b>372</b>
66.1 1. Zweck . . . . .	372
66.2 2. Geltungsbereich . . . . .	372
66.3 3. Grundsätze (Policy Statements) . . . . .	373
66.4 4. Rollen und Verantwortlichkeiten . . . . .	374
66.5 5. Ableitungen (Richtlinien/Standards/Prozesse) . . . . .	374
66.6 6. Compliance, Monitoring und Durchsetzung . . . . .	375
66.7 7. Ausnahmen . . . . .	376
66.8 8. Referenzen . . . . .	376
<b>67 Richtlinie: Sicherheitsanforderungen im Projektlebenszyklus</b>	<b>377</b>
67.1 1. Zweck und Geltungsbereich . . . . .	377
67.2 2. Projektklassifizierung . . . . .	377
67.3 3. Projektphasen und Security-Aktivitäten . . . . .	378
67.4 4. Security-by-Design-Prinzipien . . . . .	379
67.5 5. Security-Requirements . . . . .	380
67.6 6. Threat Modeling . . . . .	380
67.7 7. Security-Testing . . . . .	381
67.8 8. Compliance und Audit . . . . .	381
67.9 9. Referenzen . . . . .	381
<b>68 Anhang A: Annex A Control Mapping</b>	<b>383</b>
68.1 Zweck . . . . .	383
68.2 Geltungsbereich . . . . .	383
68.3 ISO/IEC 27001:2022 Annex A Struktur . . . . .	383
68.4 Annex A Control Mapping . . . . .	384
68.5 Amendment 1:2024 Änderungen . . . . .	407
68.6 Zusammenfassung . . . . .	407
68.7 Verwendung dieses Mappings . . . . .	408
68.8 Referenzen . . . . .	408
<b>69 Anhang B: Asset- und Systeminventar</b>	<b>409</b>
69.1 Zweck . . . . .	409
69.2 Geltungsbereich . . . . .	409
69.3 Asset-Kategorien . . . . .	409
69.4 Asset-Klassifizierung . . . . .	410
69.5 Hardware Assets . . . . .	410
69.6 Software Assets . . . . .	412
69.7 Daten Assets . . . . .	413
69.8 Netzwerk Assets . . . . .	414
69.9 Cloud Assets . . . . .	415
69.10 Physische Assets . . . . .	416
69.11 Asset Lifecycle Management . . . . .	417
69.12 Asset-Tagging und Kennzeichnung . . . . .	418

69.13	Inventarisierungsprozess . . . . .	418
69.14	Compliance und Audit . . . . .	419
69.15	Referenzen . . . . .	419
<b>70</b>	<b>Anhang C: Datenfluss und Schnittstellen</b>	<b>421</b>
70.1	Zweck . . . . .	421
70.2	Geltungsbereich . . . . .	421
70.3	Datenfluss-Kategorien . . . . .	422
70.4	Datenklassifizierung . . . . .	422
70.5	Interne Datenflüsse . . . . .	422
70.6	Externe Datenflüsse . . . . .	424
70.7	Grenzüberschreitende Datenflüsse . . . . .	425
70.8	Schnittstellen-Dokumentation . . . . .	426
70.9	Netzwerk-Architektur . . . . .	428
70.10	Datenfluss-Diagramme . . . . .	429
70.11	Risikobewertung Datenflüsse . . . . .	429
70.12	Monitoring und Logging . . . . .	430
70.13	Compliance und Datenschutz . . . . .	431
70.14	Änderungsmanagement . . . . .	431
70.15	Referenzen . . . . .	431
<b>71</b>	<b>Anhang D: Begriffe und Abkürzungen</b>	<b>433</b>
71.1	Zweck . . . . .	433
71.2	Geltungsbereich . . . . .	433
71.3	Abkürzungen . . . . .	433
71.4	Begriffsdefinitionen . . . . .	440
71.5	ISO/IEC 27001:2022 Spezifische Begriffe . . . . .	446
71.6	Referenzen . . . . .	447

## Chapter 1

# Informationssicherheits- Managementsystem Handbuch

### Dokument-Metadaten

- **Erstellt am:** 2026-02-05
  - **Autor:** Andreas Huemmer [andreas.huemmer@adminsенд.de]
  - **Version:** 0.0.2
  - **Typ:** ISMS-Handbuch
- 

ewpage

# Chapter 2

## ISMS-Leitlinie / Informationssicherheits-Policy

**Dokument-ID:** 0010

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Clause 5.2 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 2.1 1. Zweck

Diese Informationssicherheitsleitlinie definiert die strategischen Grundsätze und Verpflichtungen der **AdminSend GmbH** zum Schutz von Informationswerten. Sie bildet die Grundlage für das Information Security Management System (ISMS) nach ISO/IEC 27001:2022 und stellt sicher, dass Informationssicherheit als integraler Bestandteil aller Geschäftsprozesse verstanden und umgesetzt wird.

### 2.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Systeme und Informationen:** Alle IT-Systeme, Anwendungen, Daten und Informationsverarbeitungsprozesse
- **Personen:** Alle Mitarbeiter, Auftragnehmer, Lieferanten und Dritte mit Zugang zu Informationswerten
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen von dieser Policy sind nur über den definierten Ausnahmenprozess (siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md) zulässig.

## **2.3 3. Grundsätze (Policy Statements)**

Die AdminSend GmbH verpflichtet sich zu folgenden Grundsätzen der Informationssicherheit:

### **2.3.1 3.1 Vertraulichkeit (Confidentiality)**

Informationen werden nur autorisierten Personen, Systemen und Prozessen zugänglich gemacht. Der Zugriff erfolgt nach dem Need-to-Know-Prinzip und wird durch geeignete Zugangskontrollen geschützt.

### **2.3.2 3.2 Integrität (Integrity)**

Die Richtigkeit, Vollständigkeit und Aktualität von Informationen wird durch geeignete Kontrollen sichergestellt. Unbefugte oder unbeabsichtigte Änderungen werden verhindert und erkannt.

### **2.3.3 3.3 Verfügbarkeit (Availability)**

Informationen und IT-Systeme stehen autorisierten Nutzern bei Bedarf zur Verfügung. Geschäftskritische Systeme werden durch angemessene Redundanz- und Wiederherstellungsmaßnahmen geschützt.

### **2.3.4 3.4 Compliance und rechtliche Anforderungen**

Die Organisation erfüllt alle anwendbaren gesetzlichen, regulatorischen und vertraglichen Anforderungen an die Informationssicherheit, einschließlich Datenschutz (DSGVO), Branchenstandards und Kundenanforderungen.

### **2.3.5 3.5 Risikoorientierter Ansatz**

Informationssicherheitsmaßnahmen werden auf Basis einer systematischen Risikoanalyse priorisiert und umgesetzt. Risiken werden identifiziert, bewertet und nach definierten Kriterien behandelt.

### **2.3.6 3.6 Kontinuierliche Verbesserung**

Das ISMS wird kontinuierlich überwacht, gemessen und verbessert. Sicherheitsvorfälle, Audits und Reviews dienen als Grundlage für Verbesserungsmaßnahmen.

### **2.3.7 3.7 Awareness und Schulung**

Alle Mitarbeiter werden regelmäßig über Informationssicherheitsrisiken und ihre Verantwortlichkeiten geschult. Sicherheitsbewusstsein ist Teil der Unternehmenskultur.

### **2.3.8 3.8 Lieferanten- und Drittparteien-Management**

Lieferanten und Dritte, die Zugang zu Informationswerten haben, werden nach Sicherheitskriterien bewertet und vertraglich zur Einhaltung von Sicherheitsanforderungen verpflichtet.

## 2.4 4. Rollen und Verantwortlichkeiten

### 2.4.1 RACI-Matrix: ISMS-Leitlinie

Aktivität	CISO	CIO	Geschäftsführung	IT-Betrieb	Fachabteilungen
Policy-Erstellung	R/A	C	I	C	C
Policy-Genehmigung	C	C	A	I	I
Policy-Kommunikation	R	C	I	I	I
Policy-Umsetzung	A	R	I	R	R
Policy-Überwachung	R/A	C	I	C	C
Policy-Review	R/A	C	C	I	I

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

### 2.4.2 Schlüsselrollen

- **CISO (Chief Information Security Officer):** Thomas Weber (thomas.weber@adminsенд.de)
  - Verantwortlich für die Entwicklung, Umsetzung und Überwachung des ISMS
  - Berichtet an: Anna Schmidt
- **CIO (Chief Information Officer):** Anna Schmidt (anna.schmidt@adminsенд.de)
  - Verantwortlich für IT-Strategie und IT-Betrieb
  - Unterstützt ISMS-Umsetzung
- **Geschäftsführung:** {{ meta.management.ceo }}
  - Genehmigt ISMS-Leitlinie und stellt Ressourcen bereit
  - Trägt Gesamtverantwortung für Informationssicherheit

## 2.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Diese abstrakte Policy wird durch folgende detaillierte Dokumente konkretisiert:

### 2.5.1 Basis-ISMS-Dokumente

- 0020\_ISMS\_Geltungsbereich\_Scope.md - ISMS Scope Definition
- 0030\_ISMS\_Kontext\_und\_Interessierte\_Parteien.md - Context of Organization
- 0040\_ISMS\_Governance\_Rollen\_und\_Verantwortlichkeiten.md - ISMS Governance
- 0060\_ISMS\_Risikomanagement\_Methodik.md - Risk Management Methodology

### 2.5.2 Themenspezifische Policies (Abstract)

- 0220\_Policy\_Zugriffssteuerung\_und\_Identitätsmanagement.md
- 0240\_Policy\_Authentisierung\_und\_Passwoerter.md

- 0260\_Policy\_Kryptografie\_und\_Schluesselmanagement.md
- 0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md
- [Weitere Policies siehe ISMS-Dokumentenstruktur]

### 2.5.3 Detaillierte Richtlinien (Detailed Guidelines)

- Siehe entsprechende Richtlinien-Dokumente (0210-0690, ungerade Nummern)

## 2.6 6. Compliance, Monitoring und Durchsetzung

### 2.6.1 Messgrößen und KPIs

- Anzahl Sicherheitsvorfälle pro Quartal
- Durchschnittliche Zeit zur Behebung kritischer Schwachstellen
- Schulungsteilnahme-Quote (Ziel: 100% jährlich)
- Audit-Findings und deren Behebungsrate
- Compliance-Rate mit Sicherheitsrichtlinien

### 2.6.2 Nachweise und Evidence

- ISMS-Dokumentation und Aufzeichnungen
- Audit-Berichte (intern und extern)
- Risikoregister und Risikobehandlungspläne
- Schulungsnachweise und Awareness-Kampagnen
- Incident-Reports und Lessons Learned

### 2.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt und können zu disziplinarischen Maßnahmen führen, einschließlich:

- Verwarnung und Nachschulung
- Entzug von Zugriffsrechten
- Arbeitsrechtliche Konsequenzen
- Rechtliche Schritte bei vorsätzlichen oder grob fahrlässigen Verstößen

## 2.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig und müssen über den definierten Ausnahmenprozess beantragt werden:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und ggf. der Geschäftsführung genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert und regelmäßig überprüft
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet und müssen regelmäßig erneuert werden

## 2.8 8. Referenzen

### 2.8.1 Interne Dokumente

- ISMS-Dokumentenstruktur (siehe README.md)
- Risikoregister (0080\_ISMS\_Risikoregister\_Template.md)
- Statement of Applicability (0100\_ISMS\_Statement\_of\_Applicability\_SoA\_Template.md)
- Internes Auditprogramm (0130\_ISMS\_Internes\_Auditprogramm.md)

### 2.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 - Information security management systems - Requirements
- ISO/IEC 27001:2022/Amd 1:2024 - Amendment 1 (Annex A updates)
- ISO/IEC 27002:2022 - Information security controls
- DSGVO (EU 2016/679) - Datenschutz-Grundverordnung
- BSI IT-Grundschutz - Bundesamt für Sicherheit in der Informationstechnik

---

#### Genehmigt durch:

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

Nächster Review: {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 3

## ISMS-Geltungsbereich (Scope)

**Dokument-ID:** 0020

**Dokumenttyp:** ISMS-Grundlagendokument

**Standard-Referenz:** ISO/IEC 27001:2022 Clause 4.3

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 3.1 1. Scope-Definition

Der Geltungsbereich des Information Security Management Systems (ISMS) der **AdminSend GmbH** umfasst:

#### 3.1.1 1.1 Organisation

- **Organisationsname:** AdminSend GmbH
- **Rechtsform:** {{ meta.organization.legal\_form }}
- **Hauptsitz:** Musterstraße 123
- **Anzahl Mitarbeiter:** {{ meta.organization.employee\_count }}
- **Branche:** {{ meta.organization.industry }}

#### 3.1.2 1.2 Standorte

Das ISMS gilt für folgende Standorte:

- **Hauptstandort:** {{ netbox.site.name }}
  - Adresse: {{ netbox.site.address }}
  - Funktion: Rechenzentrum, Büros, Entwicklung

[TODO: Weitere Standorte hinzufügen]

### **3.1.3 1.3 Prozesse und Services**

Das ISMS deckt folgende Geschäftsprozesse und IT-Services ab:

**Kernprozesse:** - IT-Betrieb und Infrastrukturmanagement - Softwareentwicklung und DevOps - Datenverarbeitung und Datenmanagement - Kundenservice und Support - [TODO: Weitere Kernprozesse]

**IT-Services:** - Netzwerkinfrastruktur ({{ netbox.device.core\_switch.name }}) - Server- und Virtualisierungsplattformen - Cloud-Services und SaaS-Anwendungen - Datenbanksysteme - Backup- und Recovery-Systeme - [TODO: Weitere IT-Services]

### **3.1.4 1.4 Informationswerte und Assets**

Das ISMS schützt folgende Kategorien von Informationswerten:

**Daten und Informationen:** - Kundendaten (personenbezogene Daten gemäß DSGVO) - Geschäftsdaten (Verträge, Finanzdaten, Strategiedokumente) - Technische Daten (Quellcode, Systemdokumentation, Konfigurationen) - Mitarbeiterdaten (HR-Daten, Zugangsdaten)

**IT-Systeme und Infrastruktur:** - Produktionssysteme und Entwicklungsumgebungen - Netzwerkkomponenten (Router, Switches, Firewalls) - Endgeräte (Laptops, Workstations, Mobile Devices) - Cloud-Infrastruktur und virtuelle Maschinen

**Anwendungen und Software:** - Geschäftsanwendungen (ERP, CRM, etc.) - Entwicklungstools und CI/CD-Pipelines - Kommunikationsplattformen (E-Mail, Collaboration Tools)

### **3.1.5 1.5 Systeme und Plattformen**

Das ISMS umfasst folgende technische Plattformen:

**Netzwerkinfrastruktur:** - Core Switch: {{ netbox.device.core\_switch.name }} - Management VLAN: {{ netbox.vlan.management.vid }} - [TODO: Weitere Netzwerkkomponenten aus NetBox]

**Server und Virtualisierung:** - [TODO: Serverliste aus Asset-Inventar]

**Cloud-Plattformen:** - [TODO: AWS/Azure/GCP Accounts und Services]

**Sicherheitssysteme:** - Firewall, IDS/IPS, SIEM - Endpoint Protection (EDR/AV) - Identity and Access Management (IAM)

## **3.2 2. Scope-Grenzen und Ausschlüsse**

### **3.2.1 2.1 Ausgeschlossene Bereiche**

Folgende Bereiche sind explizit vom ISMS-Scope ausgeschlossen:

[TODO: Ausschlüsse definieren, z.B.]: - Produktionsstätten (falls nicht IT-relevant) - Externe Lieferanten-Systeme (außerhalb unserer Kontrolle) - Legacy-Systeme im Auslaufbetrieb (mit Auslaufdatum)

### **3.2.2 2.2 Begründung für Ausschlüsse**

Für jeden Ausschluss wird eine Begründung dokumentiert:

[TODO: Begründungen für Ausschlüsse] - **Beispiel:** Legacy-System XYZ wird am [Datum] außer Betrieb genommen und enthält keine kritischen Daten mehr.

### 3.2.3 2.3 Risiken und Abhängigkeiten durch Ausschlüsse

Ausschlüsse werden im Risikoregister erfasst und bewertet:

[TODO: Risikobewertung für Ausschlüsse] - Siehe 0080\_ISMS\_Risikoregister\_Template.md für Details

## 3.3 3. Schnittstellen

### 3.3.1 3.1 Externe Organisationen und Provider

Das ISMS hat Schnittstellen zu folgenden externen Parteien:

**Cloud-Provider:** - [TODO: AWS/Azure/GCP - Services und Verantwortlichkeiten]

**Managed Service Provider:** - [TODO: MSP-Partner und deren Zugriffe]

**Lieferanten und Dienstleister:** - [TODO: Kritische Lieferanten mit Zugang zu Informationsswerten]

### 3.3.2 3.2 Andere Managementsysteme

Das ISMS ist mit folgenden anderen Managementsystemen integriert:

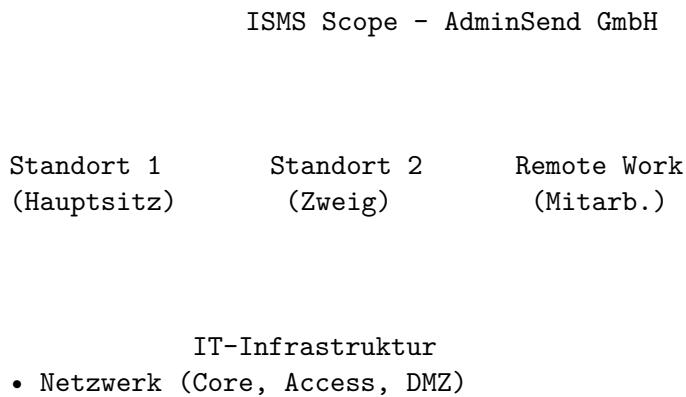
**Business Continuity Management (BCM):** - Schnittstelle zu BCM-Handbuch (siehe 0440\_Policy\_Business\_Continuity\_ICT\_Readiness.md) - Gemeinsame Risikoanalyse und BIA

**Datenschutz-Managementsystem (DSMS):** - Schnittstelle zu DSGVO-Compliance (siehe 0560\_Policy\_Datenschutz\_Schnittstellen.md) - Gemeinsame Verarbeitungsverzeichnisse und Datenschutz-Folgenabschätzungen

**Qualitätsmanagement (QMS):** - [TODO: Schnittstellen zu ISO 9001 oder anderen QMS]

## 3.4 4. Scope-Diagramm

Das folgende Diagramm visualisiert den ISMS-Geltungsbereich:



- Server (Prod, Dev, Test)
- Cloud (AWS/Azure/GCP)
- Endpoints (Laptops, Workstations, Mobile)

#### Geschäftsprozesse

- IT-Betrieb & Support
- Softwareentwicklung
- Datenverarbeitung
- Kundenservice

#### Informationswerte

- Kundendaten (DSGVO-relevant)
- Geschäftsdaten (Verträge, Finanzen)
- Technische Daten (Code, Configs)
- Mitarbeiterdaten (HR)

Externe Schnittstellen:

Cloud-Provider (AWS/Azure/GCP)

Managed Service Provider

Lieferanten und Dienstleister

Kunden und Partner

Ausschlüsse:

[TODO: Ausgeschlossene Bereiche]

[TODO: Legacy-Systeme im Auslauf]

[TODO: Detailliertes Scope-Diagramm erstellen und verlinken] - Datei: [diagrams/isms\\_scope.png](#)

## 3.5 5. Scope-Änderungen und Review

### 3.5.1 5.1 Änderungsmanagement

Änderungen am ISMS-Scope müssen über den Change-Management-Prozess erfolgen: - Siehe [0360\\_Policy\\_Change\\_und\\_Release\\_Management.md](#) - Scope-Änderungen erfordern Genehmigung durch CISO und Geschäftsführung - Auswirkungen auf Risikoanalyse und SoA müssen bewertet werden

### 3.5.2 5.2 Regelmäßiger Review

Der ISMS-Scope wird regelmäßig überprüft: - **Jährlicher Review:** Im Rahmen des Management Reviews (siehe [0140\\_ISMS\\_Management\\_Review\\_Template.md](#)) - **Anlassbezogener Review:** Bei wesentlichen organisatorischen Änderungen (Merger, Akquisitionen, neue Standorte, neue Services)

## 3.6 6. Referenzen

### 3.6.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0030\_ISMS\_Kontext\_und\_Interessierte\_Parteien.md - Context of Organization
- 0050\_ISMS\_Strukturanalyse\_Template.md - Structure Analysis (falls vorhanden)
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register
- 0100\_ISMS\_Statement\_of\_Applicability\_SoA\_Template.md - SoA

### 3.6.2 Externe Standards

- ISO/IEC 27001:2022 - Clause 4.3: Determining the scope of the ISMS
- ISO/IEC 27002:2022 - Information security controls

---

**Genehmigt durch:**

Thomas Weber, CISO

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 4

## Kontext der Organisation und interessierte Parteien

**Dokument-ID:** 0030

**Dokumenttyp:** ISMS-Grundlagendokument

**Standard-Referenz:** ISO/IEC 27001:2022 Clauses 4.1, 4.2

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 4.1 1. Kontext der Organisation

#### 4.1.1 1.1 Interne Themen

**Organisationsstruktur:** - Organisationsform: {{ meta.organization.legal\_form }} - Anzahl Mitarbeiter: {{ meta.organization.employee\_count }} - Organisationsstruktur: [TODO: Hierarchie, Abteilungen] - Standorte: {{ netbox.site.name }} und weitere

**Geschäftsprozesse:** - Kerngeschäft: {{ meta.organization.industry }} - Kritische Geschäftsprozesse: [TODO: Liste der kritischen Prozesse] - IT-Abhängigkeit: Hoch / Mittel / Niedrig

**Technologie und IT-Infrastruktur:** - IT-Strategie: [TODO: Cloud-first, Hybrid, On-Premise] - Technologie-Stack: [TODO: Haupttechnologien] - Digitalisierungsgrad: [TODO: Bewertung] - Legacy-Systeme: [TODO: Anzahl und Kritikalität]

**Unternehmenskultur:** - Sicherheitsbewusstsein: [TODO: Bewertung] - Risikobereitschaft: Konservativ / Moderat / Progressiv - Innovationskultur: [TODO: Bewertung] - Remote-Work-Anteil: [TODO: Prozentsatz]

**Ressourcen:** - IT-Budget: [TODO: Größenordnung] - Sicherheitsbudget: [TODO: Prozent vom IT-Budget] - Personalressourcen: [TODO: FTE für IT-Sicherheit] - Externe Unterstützung: [TODO: MSP, Berater]

## 4.1.2 1.2 Externe Themen

**Markt und Wettbewerb:** - Branche: {{ meta.organization.industry }} - Marktposition: [TODO: Marktführer, Challenger, Nische] - Wettbewerbsdruck: Hoch / Mittel / Niedrig - Kundenerwartungen: [TODO: Sicherheitsanforderungen]

**Regulierung und Compliance:** - DSGVO (EU 2016/679): Anwendbar - Branchenspezifische Regulierung: [TODO: z.B. KRITIS, NIS2, DORA] - Internationale Standards: ISO 27001, ISO 27002 - Vertragliche Verpflichtungen: [TODO: Kundenvorgaben]

**Bedrohungslage:** - Cyber-Bedrohungen: Ransomware, Phishing, DDoS, APT - Bedrohungskräfte: Cyberkriminelle, Hacktivisten, Nationalstaaten - Branchenspezifische Risiken: [TODO: Spezifische Bedrohungen] - Aktuelle Sicherheitsvorfälle: [TODO: Relevante Incidents in der Branche]

**Lieferketten und Abhängigkeiten:** - Cloud-Provider: [TODO: AWS, Azure, GCP] - Managed Service Provider: [TODO: MSP-Partner] - Kritische Lieferanten: [TODO: Software-Lieferanten, Hardware-Lieferanten] - Outsourcing: [TODO: Ausgelagerte Prozesse]

**Technologische Trends:** - Cloud Computing: Zunehmende Nutzung - KI und Automatisierung: [TODO: Einsatzgebiete] - IoT und OT: [TODO: Relevanz] - Mobile und Remote Work: Zunehmend

## 4.2 2. Interessierte Parteien (Stakeholders)

### 4.2.1 2.1 Stakeholder-Analyse

Partei	Erwartungen/Anforderungen	Relevanz	Nachweis/Quelle
<b>Kunden</b>	Datenschutz, Verfügbarkeit, Vertraulichkeit	Hoch	Verträge, SLAs, NDA
<b>Geschäftsführer</b>	Risikominimierung, Compliance, Business Continuity	Hoch	Unternehmensstrategie
<b>Mitarbeitende</b>	Sichere Arbeitsumgebung, Datenschutz, Schulung	Hoch	HR-Policy, Betriebsrat
<b>Aufsichtsbehörden</b>	DSGVO-Compliance, Meldepflichten	Hoch	DSGVO, NIS2, KRITIS
<b>Lieferanten/Plaeranten</b>	Qualitätsstandards, Vertraulichkeit	Mittel	Verträge, SLAs
<b>Investoren/Eigentümer</b>	Erfolg, Reputation	Mittel	Geschäftsberichte
<b>Versicherungen</b>	Sicherheitsmaßnahmen, Incident Response	Mittel	Cyber-Versicherung
<b>Öffentlichkeit/Medien</b>	Transparenz, Vertrauen	Niedrig	PR-Strategie

### 4.2.2 2.2 Detaillierte Stakeholder-Anforderungen

**Kunden:** - Anforderungen: Datenschutz (DSGVO), Verfügbarkeit (99,9% SLA), Vertraulichkeit (NDA) - Kommunikation: Regelmäßige Security Updates, Incident Notifications - Nachweise: SOC 2, ISO 27001 Zertifikat, Penetration Test Reports

**Aufsichtsbehörden:** - Anforderungen: DSGVO-Compliance, Meldepflichten (72h), Datenschutz-Folgenabschätzung - Kommunikation: Incident Reporting, Audit-Kooperation - Nachweise: Verarbeitungsverzeichnis, DSFA, Incident Reports

**Mitarbeitende:** - Anforderungen: Sichere Arbeitsumgebung, Datenschutz, Schulung - Kommunikation: Security Awareness Training, Policy Communication - Nachweise: Schulungsnachweise, Awareness-Kampagnen

**Lieferanten und Partner:** - Anforderungen: Sicherheitsstandards, Vertraulichkeit, Incident Notification - Kommunikation: Security Requirements in Contracts, Regular Reviews - Nachweise: Third-Party Risk Assessments, Security Questionnaires

## 4.3 3. Anforderungen an das ISMS

### 4.3.1 3.1 Compliance-Anforderungen (Legal/Regulatorik)

**Datenschutz:** - **DSGVO (EU 2016/679):** Datenschutz-Grundverordnung - Anforderungen: Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung - Umsetzung: Siehe 0560\_Policy\_Datenschutz\_Schnittstellen.md - Nachweise: Verarbeitungsverzeichnis, DSFA, Datenschutzerklärung

**Branchenspezifische Regulierung:** - [TODO: KRITIS, NIS2, DORA, PCI-DSS, HIPAA, etc.] - Anforderungen: [TODO: Spezifische Anforderungen] - Umsetzung: [TODO: Verweis auf relevante Policies]

**Arbeitsrecht und Betriebsrat:** - Mitbestimmung bei IT-Sicherheitsmaßnahmen - Datenschutz für Mitarbeiterdaten - Umsetzung: Siehe 0520\_Policy\_HR\_Security.md

### 4.3.2 3.2 Vertragliche Anforderungen

**Kundenverträge:** - SLAs: Verfügbarkeit, Performance, Support - Sicherheitsanforderungen: Verschlüsselung, Zugriffskontrolle, Audit-Rechte - Zertifizierungen: ISO 27001, SOC 2, etc. - Incident Notification: Meldepflichten bei Sicherheitsvorfällen

**Lieferantenverträge:** - Security Requirements: Siehe 0460\_Policy\_Lieferanten\_und\_Cloud\_Sicherheit.md - SLAs und OLAs: Service Level Agreements - Audit-Rechte: Right to Audit Clauses

**Versicherungsverträge:** - Cyber-Versicherung: Mindestanforderungen an Sicherheitsmaßnahmen - Meldepflichten: Incident Reporting an Versicherung

### 4.3.3 3.3 Interne Anforderungen

**Geschäftsleitung:** - Risikomanagement: Akzeptable Risikoniveaus definieren - Business Continuity: RTO/RPO-Vorgaben - Compliance: Einhaltung aller gesetzlichen und vertraglichen Verpflichtungen

**IT-Strategie:** - Cloud-First-Strategie: Sicherheitsanforderungen für Cloud-Services - DevOps und Agile: Security in DevOps (DevSecOps) - Innovation: Balance zwischen Innovation und Sicherheit

**Interne Policies:** - Siehe ISMS-Dokumentenstruktur (Policies 0200-0680) - Detaillierte Richtlinien (Guidelines 0210-0690)

## 4.4 4. Auswirkungen auf das ISMS

### 4.4.1 4.1 Ableitung von ISMS-Zielen

Aus dem Kontext und den Stakeholder-Anforderungen werden folgende ISMS-Ziele abgeleitet:

1. **Compliance:** Einhaltung aller gesetzlichen und vertraglichen Anforderungen
2. **Risikomanagement:** Identifikation und Behandlung von Informationssicherheitsrisiken
3. **Business Continuity:** Sicherstellung der Geschäftskontinuität bei Sicherheitsvorfällen
4. **Awareness:** Förderung des Sicherheitsbewusstseins bei allen Mitarbeitenden
5. **Kontinuierliche Verbesserung:** Regelmäßige Überprüfung und Verbesserung des ISMS

Siehe 0110\_ISMS\_Sicherheitsziele\_und\_Metriken.md für detaillierte Ziele und KPIs.

### 4.4.2 4.2 Auswirkungen auf Risikoanalyse

Der Kontext und die Stakeholder-Anforderungen fließen in die Risikoanalyse ein: - Siehe 0060\_ISMS\_Risikomanagement\_Methodik.md - Siehe 0080\_ISMS\_Risikoregister\_Template.md

### 4.4.3 4.3 Auswirkungen auf Statement of Applicability (SoA)

Die Anforderungen beeinflussen die Auswahl und Begründung von Annex A Controls: - Siehe 0100\_ISMS\_Statement\_of\_Applicability\_SoA\_Template.md

## 4.5 5. Review und Aktualisierung

### 4.5.1 5.1 Regelmäßiger Review

Der Kontext und die Stakeholder-Anforderungen werden regelmäßig überprüft: - **Jährlicher Review:** Im Rahmen des Management Reviews - **Anlassbezogener Review:** Bei wesentlichen Änderungen (neue Regulierung, neue Stakeholder, Merger/Akquisition)

### 4.5.2 5.2 Änderungsmanagement

Änderungen am Kontext oder an Stakeholder-Anforderungen werden dokumentiert und bewertet:  
- Auswirkungen auf ISMS-Scope, Risikoanalyse und SoA - Change-Management-Prozess: Siehe 0360\_Policy\_Change\_und\_Release\_Management.md

## 4.6 6. Referenzen

### 4.6.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0020\_ISMS\_Geltungsbereich\_Scope.md - ISMS Scope
- 0060\_ISMS\_Risikomanagement\_Methodik.md - Risk Management
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register
- 0100\_ISMS\_Statement\_of\_Applicability\_SoA\_Template.md - SoA
- 0110\_ISMS\_Sicherheitsziele\_und\_Metriken.md - Security Objectives

#### **4.6.2 Externe Standards**

- **ISO/IEC 27001:2022** - Clause 4.1: Understanding the organization and its context
  - **ISO/IEC 27001:2022** - Clause 4.2: Understanding the needs and expectations of interested parties
  - **DSGVO (EU 2016/679)** - Datenschutz-Grundverordnung
- 

**Genehmigt durch:**

Thomas Weber, CISO

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 5

## ISMS-Governance: Rollen und Verantwortlichkeiten

**Dokument-ID:** 0040

**Dokumenttyp:** ISMS-Grundlagendokument

**Standard-Referenz:** ISO/IEC 27001:2022 Clause 5.3

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 5.1 1. ISMS-Governance-Struktur

#### 5.1.1 1.1 Governance-Übersicht

Die ISMS-Governance der **AdminSend GmbH** ist in die Gesamtorganisation integriert und stellt sicher, dass Informationssicherheit auf allen Ebenen verankert ist.

Geschäftsführung / Top Management  
({{ meta.management.ceo }})

CIO  
Anna Schmidt

CISO  
Thomas Weber

ISMS Manager      Security  
Team

Informationssicherheitsgremium  
(Security Steering Committee)

- CISO (Vorsitz)
- CIO
- Vertreter Fachabteilungen
- IT-Betrieb
- Datenschutzbeauftragter
- Internal Audit (beratend)

### 5.1.2 1.2 Schlüsselgremien

**Informationssicherheitsgremium (Security Steering Committee):** - **Vorsitz:** Thomas Weber (CISO) - **Mitglieder:** CIO, Vertreter Fachabteilungen, IT-Betrieb, Datenschutzbeauftragter - **Frequenz:** Quartalsweise oder anlassbezogen - **Aufgaben:** - Strategische Ausrichtung des ISMS - Genehmigung von Sicherheitsrichtlinien - Überwachung der ISMS-Performance - Entscheidung über Risikoakzeptanz - Budget-Freigabe für Sicherheitsmaßnahmen

### 5.1.3 1.3 Schnittstellen zu anderen Funktionen

**IT Service Management (ITSM):** - Integration von Security in ITIL-Prozesse - Incident Management, Change Management, Problem Management - Kontakt: {{ meta.it.service\_manager }}

**Datenschutz (DSMS):** - Schnittstelle zu DSGVO-Compliance - Gemeinsame Risikoanalyse und Datenschutz-Folgenabschätzung - Kontakt: {{ meta.privacy.dpo }}

**Risk Management:** - Integration in Enterprise Risk Management (ERM) - Gemeinsames Risiko-register - Kontakt: {{ meta.risk.manager }}

**Business Continuity Management (BCM):** - Schnittstelle zu BCM-Handbuch - Gemeinsame BIA und Notfallplanung - Kontakt: {{ meta.bcm.manager }}

**Internal Audit:** - Unabhängige Prüfung des ISMS - Audit-Planung und -Durchführung - Kontakt: {{ meta.audit.manager }}

## 5.2 2. Rollenbeschreibungen

### 5.2.1 2.1 Geschäftsführung / Top Management

**Rolle:** {{ meta.management.ceo }}

**Verantwortlichkeiten:** - Gesamtverantwortung für Informationssicherheit - Genehmigung der ISMS-Leitlinie - Bereitstellung von Ressourcen für das ISMS - Förderung der Sicherheitskultur - Teilnahme am Management Review

**Befugnisse:** - Genehmigung von Sicherheitsbudgets - Entscheidung über strategische Sicherheitsinitiativen - Genehmigung von Risikoakzeptanzen (bei hohen Risiken)

### 5.2.2 2.2 CISO (Chief Information Security Officer)

**Rolle:** Thomas Weber (thomas.weber@adminsенд.de)

**Verantwortlichkeiten:** - Entwicklung, Implementierung und Überwachung des ISMS - Leitung des Informationssicherheitsremiums - Erstellung und Pflege von Sicherheitsrichtlinien - Durchführung von Risikoanalysen - Incident Response Koordination - Reporting an Geschäftsführung - Awareness und Schulung

**Befugnisse:** - Genehmigung von Sicherheitsrichtlinien - Anordnung von Sicherheitsmaßnahmen - Eskalation bei kritischen Sicherheitsvorfällen - Zugriff auf alle sicherheitsrelevanten Informationen

**Berichtslinie:** Berichtet an Anna Schmidt (CIO) und Geschäftsführung

### 5.2.3 2.3 CIO (Chief Information Officer)

**Rolle:** Anna Schmidt (anna.schmidt@adminsенд.de)

**Verantwortlichkeiten:** - IT-Strategie und IT-Betrieb - Unterstützung der ISMS-Umsetzung - Bereitstellung von IT-Ressourcen für Sicherheitsmaßnahmen - Integration von Security in IT-Prozesse

**Befugnisse:** - Genehmigung von IT-Projekten mit Sicherheitsrelevanz - Ressourcenzuteilung für IT-Sicherheit

### 5.2.4 2.4 ISMS Manager

**Rolle:** [TODO: Name und Kontakt]

**Verantwortlichkeiten:** - Operative Umsetzung des ISMS - Pflege der ISMS-Dokumentation - Koordination von Audits und Reviews - Tracking von Maßnahmen und Findings - Unterstützung des CISO

**Befugnisse:** - Koordination von ISMS-Aktivitäten - Anforderung von Informationen für Audits

### 5.2.5 2.5 Asset Owner / Process Owner

**Rolle:** Fachabteilungsleiter, Prozessverantwortliche

**Verantwortlichkeiten:** - Verantwortung für Informationswerte in ihrem Bereich - Klassifizierung von Informationen - Definition von Zugriffsrechten - Umsetzung von Sicherheitsmaßnahmen in ihrem Bereich - Meldung von Sicherheitsvorfällen

**Befugnisse:** - Genehmigung von Zugriffsrechten für ihre Assets - Entscheidung über Sicherheitsmaßnahmen in ihrem Bereich

### 5.2.6 2.6 Control Owner

**Rolle:** Verantwortliche für spezifische Sicherheitskontrollen

**Verantwortlichkeiten:** - Implementierung und Betrieb von Sicherheitskontrollen - Nachweis der Wirksamkeit (Evidence) - Reporting über Control-Status - Behebung von Control-Deficiencies

**Befugnisse:** - Umsetzung von Sicherheitsmaßnahmen im Rahmen ihrer Kontrolle

**Beispiele:** - Patch Management Control Owner: IT-Betrieb - Access Control Owner: IAM-Team - Backup Control Owner: Backup-Administrator

### 5.2.7 2.7 IT-Betrieb

**Rolle:** IT-Operations-Team

**Verantwortlichkeiten:** - Umsetzung technischer Sicherheitsmaßnahmen - Monitoring und Alerting - Incident Response (technisch) - Patch Management - Backup und Recovery

**Befugnisse:** - Durchführung von Sicherheitsmaßnahmen - Notfall-Zugriffe bei Incidents

### 5.2.8 2.8 Mitarbeitende (alle)

**Rolle:** Alle Mitarbeiter, Auftragnehmer, Dritte

**Verantwortlichkeiten:** - Einhaltung von Sicherheitsrichtlinien - Meldung von Sicherheitsvorfällen - Teilnahme an Security Awareness Training - Schutz von Zugangsdaten und Informationen

**Befugnisse:** - Zugriff auf Informationen nach Need-to-Know-Prinzip

### 5.2.9 2.9 Internal Audit / Compliance

**Rolle:** {{ meta.audit.manager }}

**Verantwortlichkeiten:** - Unabhängige Prüfung des ISMS - Audit-Planung und -Durchführung - Reporting von Audit-Findings - Überwachung der Maßnahmenumsetzung

**Befugnisse:** - Zugriff auf alle ISMS-relevanten Informationen - Anforderung von Nachweisen und Interviews

## 5.3 3. RACI-Matrix: ISMS-Prozesse

### 5.3.1 3.1 ISMS-Kernprozesse

Aktivität	CISO	CIO	ISMS Manager	Asset Owner	IT-Betrieb	Internal Audit
ISMS-Strategie entwickeln	R/A	C	C	I	I	I
Policies erstellen	R/A	C	R	C	C	I
Risikoanalyse durchführen	A	C	R	C	C	I
Risikobehandlung planen	C	R	C	R	I	
SoA pflegen	A	I	R	C	C	I

Aktivität	CISO	CIO	ISMS Manager	Asset Owner	IT-Betrieb	Internal Audit
<b>Controls imple-mentieren</b>	A	C	C	R	R	I
<b>Monitoring durch-führen</b>	A	I	C	I	R	I
<b>Incidents managen</b>	A	C	C	I	R	I
<b>Audits durch-führen</b>	C	C	C	C	C	R/A
<b>Management Review</b>	R	C	R	I	I	C
<b>Awareness Training</b>	A	C	R	I	I	I

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

### 5.3.2 3.2 Annex A Controls (Beispiele)

Control	Control Owner	Responsible	Accountable	Consulted	Informed
<b>A.5.1 Policies</b>	CISO	ISMS Manager	CISO	CIO, Fachabt.	Alle
<b>A.5.7 Threat Intelligence</b>	Security Team	Security Analyst	CISO	IT-Betrieb	ISMS Manager
<b>A.5.10 Acceptable Use</b>	CISO	HR	CISO	IT-Betrieb	Alle
<b>A.5.15 Access Control</b>	IAM Team	IAM Admin	CIO	CISO	IT-Betrieb
<b>A.5.23 Cloud Services</b>	Cloud Architect	Cloud Admin	CIO	CISO	IT-Betrieb
<b>A.8.8 Backup</b>	IT-Betrieb	Backup Admin	CIO	CISO	ISMS Manager
<b>A.8.16 Monitoring</b>	Security Team	SOC Analyst	CISO	IT-Betrieb	ISMS Manager

## **5.4 4. Eskalationspfade**

### **5.4.1 4.1 Sicherheitsvorfälle**

Incident Detection

IT-Betrieb / SOC

CISO (bei kritischen Incidents)

CIO / Geschäftsführung (bei Major Incidents)

Externe Meldung (Behörden, Kunden)

Siehe 0400\_Policy\_Incident\_Management.md für Details.

### **5.4.2 4.2 Risikoakzeptanz**

Risikoidentifikation

CISO (Risikobewertung)

CISO (Risikoakzeptanz bei niedrigen/mittleren Risiken)

Geschäftsführung (Risikoakzeptanz bei hohen Risiken)

Siehe 0070\_ISMS\_Risikoakzeptanzkriterien.md für Details.

## **5.5 5. Referenzen**

### **5.5.1 Interne Dokumente**

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0030\_ISMS\_Kontext\_und\_Interessierte\_Parteien.md - Context
- 0060\_ISMS\_Risikomanagement\_Methodik.md - Risk Management
- 0130\_ISMS\_Internes\_Auditprogramm.md - Internal Audit Program

### **5.5.2 Externe Standards**

- ISO/IEC 27001:2022 - Clause 5.3: Organizational roles, responsibilities and authorities
- ISO/IEC 27002:2022 - Control 5.2: Information security roles and responsibilities

**Genehmigt durch:**

`{{ meta.management.ceo }}`, Geschäftsführung

Datum: `{{ meta.document.approval_date }}`

**Nächster Review:** `{{ meta.document.next_review }}`

ewpage

# Chapter 6

# Dokumentenlenkung / Dokumentierte Information

**Dokument-ID:** 0050

**Dokumenttyp:** ISMS-Grundlagendokument

**Standard-Referenz:** ISO/IEC 27001:2022 Clause 7.5

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

## 6.1 1. Zweck und Geltungsbereich

Dieses Dokument definiert die Anforderungen an die Lenkung dokumentierter Informationen im Rahmen des ISMS der **AdminSend GmbH**. Es stellt sicher, dass:

- Dokumente verfügbar und geeignet für die Verwendung sind
- Dokumente angemessen geschützt werden
- Dokumente kontrolliert erstellt, geprüft, genehmigt und aktualisiert werden

## 6.2 2. Ablage und Zugriff

### 6.2.1 2.1 Offizieller Ablageort

**Primärer Ablageort:** - **System:** [TODO: SharePoint, Confluence, DMS] - **Pfad:** [TODO: /ISMS/Dokumentation/] - **URL:** [TODO: <https://docs.organization.com/isms/>]

**Backup und Archivierung:** - **Backup-System:** {{ netbox.backup.system }} - **Backup-Frequenz:** Täglich - **Archivierungsdauer:** 10 Jahre nach Außerbetriebnahme

### 6.2.2 2.2 Zugriffskontrolle

**Zugriffsberechtigungen:**

Dokumenttyp	CISO	ISMS Manager	IT-Betrieb	Fachabteilungen	Alle Mitarbeiter
ISMS-Leitlinie	R/W	R/W	R	R	R
Policies (Abstract)	R/W	R/W	R	R	R
Richtlinien (Detailed)	R/W	R/W	R/W	R	R
Risikoregister	R/W	R/W	R	-	-
Audit-Berichte	R/W	R/W	-	-	-
Incident Reports	R/W	R/W	R/W	-	-

**Legende:** R = Read (Lesen), W = Write (Schreiben), - = Kein Zugriff

**Zugriffsverwaltung:** - Zugriffsrechte werden über IAM-System verwaltet - Siehe 0220\_Policy\_Zugriffssteuerung  
- Rezertifizierung: Quartalsweise

### 6.2.3 2.3 Offline-/Notfallzugriff

**Notfallzugriff:** - Kritische Dokumente (Notfallpläne, Kontaktlisten) werden zusätzlich offline gespeichert - Ablageort: [TODO: Physischer Safe, verschlüsselter USB-Stick] - Verantwortlich: Thomas Weber

**Break-Glass-Zugriff:** - Siehe 0200\_Notfallzugang\_BreakGlass.md (BCM-Handbuch) - Notfallzugriff auf ISMS-Dokumentation bei Ausfall des primären Systems

## 6.3 3. Dokumentenlebenszyklus

### 6.3.1 3.1 Erstellung

**Prozess:** 1. **Initiierung:** Bedarf wird identifiziert (z.B. neue Policy, neue Anforderung) 2. **Autor benennen:** CISO oder ISMS Manager benennt Autor 3. **Template verwenden:** Autor verwendet entsprechendes Template 4. **Entwurf erstellen:** Autor erstellt Entwurf mit Status "Entwurf" 5. **Metadaten erfassen:** Dokument-ID, Owner, Version, Klassifizierung

**Verantwortlich:** Dokumentautor (benannt durch CISO)

### 6.3.2 3.2 Review

**Review-Prozess:** 1. **Peer Review:** Fachliche Prüfung durch Kollegen 2. **Stakeholder Review:** Konsultation betroffener Stakeholder 3. **CISO Review:** Finale Prüfung durch CISO 4. **Status ändern:** Von "Entwurf" zu "In Review"

**Review-Kriterien:** - Fachliche Korrektheit - Vollständigkeit - Konsistenz mit anderen ISMS-Dokumenten - Compliance mit ISO 27001:2022 - Verständlichkeit und Umsetzbarkeit

**Verantwortlich:** CISO oder ISMS Manager

### 6.3.3 3.3 Freigabe

**Freigabe-Prozess:** 1. **Freigabe-Antrag:** Nach erfolgreichem Review 2. **Genehmigung:** Durch CISO (Policies) oder Geschäftsführung (ISMS-Leitlinie) 3. **Status ändern:** Von "In Review" zu "Freigegeben" 4. **Versionsnummer:** Finale Versionsnummer vergeben (z.B. 1.0)

**Freigabe-Befugnisse:**

Dokumenttyp	Freigabe durch
ISMS-Leitlinie	Geschäftsführung
Policies (Abstract)	CISO
Richtlinien (Detailed)	CISO oder ISMS Manager
Prozessdokumente	CISO oder ISMS Manager
Templates	ISMS Manager

**Verantwortlich:** Siehe Tabelle oben

### 6.3.4 3.4 Veröffentlichung und Kommunikation

**Veröffentlichung:** 1. **Upload:** Dokument wird im offiziellen Ablageort veröffentlicht 2. **Dokumentenregister aktualisieren:** Eintrag im Dokumentenregister 3. **Alte Version archivieren:** Vorherige Version wird archiviert

**Kommunikation:** - **Neue Dokumente:** E-Mail-Benachrichtigung an alle betroffenen Stakeholder  
- **Wesentliche Änderungen:** E-Mail-Benachrichtigung + Awareness-Kampagne - **Kleinere Änderungen:** Eintrag im Change-Log, keine separate Benachrichtigung

**Kommunikationskanäle:** - E-Mail an alle Mitarbeiter - Intranet-News - Security Awareness Training - Team-Meetings

**Verantwortlich:** ISMS Manager

### 6.3.5 3.5 Änderungsmanagement

**Änderungsprozess:** 1. **Änderungsantrag:** Bedarf für Änderung wird identifiziert 2. **Impact Assessment:** Auswirkungen der Änderung bewerten 3. **Änderung durchführen:** Dokument wird aktualisiert 4. **Review und Freigabe:** Wie bei Neuerstellung 5. **Versionsnummer erhöhen:** Major (1.0 → 2.0) oder Minor (1.0 → 1.1)

**Versionierungsschema:** - **Major Version (X.0):** Wesentliche Änderungen, neue Anforderungen  
- **Minor Version (X.Y):** Kleinere Änderungen, Korrekturen, Klarstellungen

**Change-Log:** Jedes Dokument enthält einen Change-Log mit: - Versionsnummer - Datum - Autor  
- Beschreibung der Änderung - Genehmiger

**Verantwortlich:** Dokumentautor, CISO

### 6.3.6 3.6 Regelmäßiger Review

**Review-Intervalle:**

Dokumenttyp	Review-Intervall
ISMS-Leitlinie	Jährlich
Policies (Abstract)	Jährlich
Richtlinien (Detailed)	Jährlich oder bei Bedarf
Risikoregister	Quartalsweise
SoA	Jährlich oder bei Scope-Änderung
Prozessdokumente	Alle 2 Jahre

**Review-Trigger (anlassbezogen):** - Neue gesetzliche Anforderungen - Wesentliche organisatorische Änderungen - Sicherheitsvorfälle mit Lessons Learned - Audit-Findings - Technologieänderungen

**Review-Prozess:** 1. **Review-Erinnerung:** ISMS Manager erinnert Owner 2. **Review durchführen:** Owner prüft Aktualität und Relevanz 3. **Entscheidung:** Keine Änderung / Änderung erforderlich 4. **Dokumentation:** Review-Datum im Dokument aktualisieren

**Verantwortlich:** Dokumentowner (siehe Dokumentenregister)

### 6.3.7 3.7 Archivierung und Löschung

**Archivierung:** - **Alte Versionen:** Werden archiviert, sobald neue Version freigegeben wird - **Archivierungsdauer:** 10 Jahre - **Archivierungsort:** [TODO: Archiv-System]

**Löschung:** - **Außerbetriebnahme:** Dokumente werden nach Ablauf der Archivierungsdauer gelöscht - **Löschprozess:** Sichere Löschung gemäß 0580\_Policy\_Aufbewahrung\_und\_Loeschung.md - **Genehmigung:** Löschung muss durch CISO genehmigt werden

**Verantwortlich:** ISMS Manager

## 6.4 4. Versionierung

### 6.4.1 4.1 Versionierungsschema

**Format:** X.Y

- **X (Major Version):** Wesentliche Änderungen
  - Neue Anforderungen
  - Strukturelle Änderungen
  - Änderung des Geltungsbereichs
- **Y (Minor Version):** Kleinere Änderungen
  - Korrekturen
  - Klarstellungen
  - Aktualisierung von Kontaktdataen

**Beispiele:** - 0.1 → Entwurf - 1.0 → Erste freigegebene Version - 1.1 → Kleinere Korrektur - 2.0 → Wesentliche Überarbeitung

### 6.4.2 4.2 Change-Log

Jedes Dokument enthält einen Change-Log am Ende:

## ## Änderungshistorie

Version	Datum	Autor	Beschreibung	Genehmigt durch
1.0	2026-01-15	Thomas Weber	Initiale Version	Geschäftsführung
1.1	2026-03-20	ISMS Manager	Kontaktdaten aktualisiert	CISO
2.0	2026-12-01	Thomas Weber	Neue Anforderungen aus NIS2	Geschäftsführung

## 6.5 5. Dokumentenregister

Das Dokumentenregister ist die zentrale Übersicht aller ISMS-Dokumente.

### 6.5.1 5.1 Dokumentenregister-Struktur

Dokument-ID	Dokumenttitel	Owner	Status	Version	Letzte Änderung	Nächster Review
0010	ISMS-Leitlinie	Thomas Weber	Freigegeben	0	{} meta.document.datum	{} meta.document.next_review
0020	ISMS-Geltungsbereich	Thomas Weber	Freigegeben	0	{} meta.document.datum	{} meta.document.next_review
0030	Kontext und Stakeholder	Thomas Weber	Freigegeben	0	{} meta.document.datum	{} meta.document.next_review
0040	ISMS-Governance	Thomas Weber	Freigegeben	0	{} meta.document.datum	{} meta.document.next_review
0050	Dokumentenlenkung	Thomas Weber	Freigegeben	0	{} meta.document.datum	{} meta.document.next_review
...	...	...	...	...	...	...

[TODO: Vollständiges Dokumentenregister erstellen und pflegen]

### 6.5.2 5.2 Pflege des Dokumentenregisters

**Verantwortlich:** ISMS Manager

**Aktualisierung:** - Bei jeder Dokumentänderung - Bei Statusänderungen - Bei Owner-Wechsel

**Zugriff:** - Dokumentenregister ist für alle Mitarbeiter lesbar - Ablageort: [TODO: Link zum Dokumentenregister]

## 6. Dokumentklassifizierung

Alle ISMS-Dokumente werden klassifiziert gemäß 0280\_Policy\_Datenklassifizierung\_und\_Informationshandlung

Klassifizierung	Beschreibung	Beispiele
<b>Öffentlich</b>	Keine Vertraulichkeit	Öffentliche Policies
<b>Intern</b>	Nur für Mitarbeiter	Die meisten ISMS-Dokumente
<b>Vertraulich</b>	Eingeschränkter Zugriff	Risikoregister, Audit-Berichte
<b>Streng vertraulich</b>	Sehr eingeschränkter Zugriff	Incident Reports mit sensiblen Daten

**Kennzeichnung:** - Klassifizierung wird im Dokument-Header angegeben - Klassifizierung bestimmt Zugriffsrechte und Handhabung

## 6.7 7. Externe Dokumente

Externe Dokumente (z.B. Lieferanten-Policies, Zertifikate) werden ebenfalls kontrolliert:

**Prozess:** 1. **Identifikation:** Relevante externe Dokumente identifizieren 2. **Bewertung:** Relevanz und Vertrauenswürdigkeit prüfen 3. **Ablage:** In separatem Bereich ablegen 4. **Kennzeichnung:** Als "Externes Dokument" kennzeichnen 5. **Review:** Regelmäßig auf Aktualität prüfen

**Verantwortlich:** ISMS Manager

## 6.8 8. Aufbewahrungsfristen

Dokumenttyp	Aufbewahrungsfrist	Rechtsgrundlage
ISMS-Leitlinie	10 Jahre nach Außerbetriebnahme	ISO 27001
Policies und Richtlinien	10 Jahre nach Außerbetriebnahme	ISO 27001
Risikoregister	10 Jahre	ISO 27001
Audit-Berichte	10 Jahre	ISO 27001, Handelsrecht
Incident Reports	10 Jahre	DSGVO, NIS2
Schulungsnachweise	10 Jahre	Nachweispflicht
Verträge	Gemäß Vertragsrecht	Handelsrecht

Siehe 0580\_Policy\_Aufbewahrung\_und\_Loeschung.md für Details.

## 6.9 9. Referenzen

### 6.9.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0040\_ISMS\_Governance\_Rollen\_und\_Verantwortlichkeiten.md - Governance
- 0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md - Data Classification
- 0360\_Policy\_Change\_und\_Release\_Management.md - Change Management
- 0580\_Policy\_Aufbewahrung\_und\_Loeschung.md - Retention and Deletion

## 6.9.2 Externe Standards

- ISO/IEC 27001:2022 - Clause 7.5: Documented information
  - ISO/IEC 27002:2022 - Control 5.1: Policies for information security
- 

**Genehmigt durch:**

Thomas Weber, CISO

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 7

## Risikomanagement – Methodik

**Dokument-ID:** 0060

**Dokumenttyp:** ISMS-Grundlagendokument

**Standard-Referenz:** ISO/IEC 27001:2022 Clause 6.1.2

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 7.1 1. Ziel und Geltungsbereich

#### 7.1.1 1.1 Ziel

Diese Methodik definiert, wie die **AdminSend GmbH** Informationssicherheitsrisiken systematisch identifiziert, bewertet, behandelt und überwacht. Sie stellt sicher, dass: - Risiken konsistent und nachvollziehbar bewertet werden - Risikobehandlungsmaßnahmen priorisiert werden - Risiken auf ein akzeptables Niveau reduziert werden - Die Geschäftsführung informierte Entscheidungen treffen kann

#### 7.1.2 1.2 Geltungsbereich

Diese Methodik gilt für alle Informationssicherheitsrisiken im ISMS-Scope (siehe 0020\_ISMS\_Geltungsbereich\_Sco...  
- IT-Systeme und Infrastruktur - Geschäftsprozesse - Informationswerte und Daten - Lieferanten  
und Drittparteien - Physische Sicherheit

### 7.2 2. Risikoobjekte

#### 7.2.1 2.1 Assets (Informationswerte)

**Kategorien:** - **Informationen und Daten:** Kundendaten, Geschäftsdaten, technische Daten,

Mitarbeiterdaten - **IT-Systeme:** Server, Netzwerkkomponenten, Endgeräte, Cloud-Infrastruktur -

**Anwendungen:** Geschäftsanwendungen, Entwicklungstools, Kommunikationsplattformen - **Services:** IT-Services, Geschäftsservices - **Personen:** Mitarbeiter mit kritischem Wissen - **Physische Assets:** Rechenzentren, Büros, Hardware

**Asset-Inventar:** - Siehe 0720\_Anhang\_Asset\_und\_Systeminventar\_Template.md - Asset-Eigentümer (Asset Owner) sind verantwortlich für ihre Assets

## 7.2.2 2.2 Geschäftsprozesse

**Kritische Geschäftsprozesse:** - [TODO: Liste der kritischen Geschäftsprozesse] - Siehe Business Impact Analysis (BIA) im BCM-Handbuch

**Prozess-Eigentümer:** - Verantwortlich für Risiken in ihrem Prozess - Siehe 0040\_ISMS\_Governance\_Rollen\_und\_

## 7.2.3 2.3 Lieferanten und Outsourcing

**Kritische Lieferanten:** - Cloud-Provider (AWS, Azure, GCP) - Managed Service Provider - Software-Lieferanten - Siehe 0460\_Policy\_Lieferanten\_und\_Cloud\_Sicherheit.md

**Third-Party Risk Assessment:** - Separate Risikobewertung für kritische Lieferanten - Siehe 0470\_Richtlinie\_Third\_Party\_Risk\_Assessment\_und\_Cloud\_Controls.md

## 7.3 3. Risikomanagement-Methodik

### 7.3.1 3.1 Risikomanagement-Prozess

#### Risikomanagement-Zyklus

1. Risikoidentifikation  
(Bedrohungen + Schwachstellen)

2. Risikobewertung  
(Wahrscheinlichkeit × Impact)

3. Risikobehandlung  
(Vermeiden, Reduzieren,  
Übertragen, Akzeptieren)

#### 4. Risikoüberwachung (Monitoring, Review)

Kontinuierliche  
Verbesserung

### 7.3.2 3.2 Risikoidentifikation

**Methoden:** 1. **Asset-basiert:** Identifikation von Bedrohungen und Schwachstellen für jedes Asset 2. **Szenario-basiert:** Analyse von Bedrohungsszenarien (z.B. Ransomware, DDoS, Insider-Bedrohung) 3. **Compliance-basiert:** Identifikation von Compliance-Risiken (DSGVO, NIS2, etc.)

**Risikoformel:**

$$\text{Risiko} = \text{Bedrohung} \times \text{Schwachstelle} \times \text{Asset-Wert}$$

**Bedrohungen (Threats):** - **Cyber-Bedrohungen:** Ransomware, Phishing, DDoS, APT, Malware - **Menschliche Bedrohungen:** Insider-Bedrohung, Social Engineering, Fehler - **Umweltbedrohungen:** Feuer, Wasser, Stromausfall, Naturkatastrophen - **Technische Bedrohungen:** Hardware-Ausfall, Software-Bugs, Konfigurationsfehler

**Schwachstellen (Vulnerabilities):** - **Technische Schwachstellen:** Ungepatchte Systeme, Fehlkonfigurationen, schwache Verschlüsselung - **Organisatorische Schwachstellen:** Fehlende Policies, unzureichende Schulung, schwache Prozesse - **Physische Schwachstellen:** Unzureichender Zutrittsschutz, fehlende Redundanz

**Quellen für Risikoidentifikation:** - Threat Intelligence (CERT, MITRE ATT&CK, Vendor Advisories) - Vulnerability Scans (CVE, CVSS) - Penetration Tests - Security Incidents und Lessons Learned - Audit-Findings - Compliance-Anforderungen

### 7.3.3 3.3 Risikobewertung

**Bewertungsskalen:**

**Wahrscheinlichkeit (Likelihood):**

Stufe	Beschreibung	Häufigkeit
1 - Sehr unwahrscheinlich	Ereignis ist theoretisch möglich, aber sehr unwahrscheinlich	< 1 in 10 Jahren
2 - Unwahrscheinlich	Ereignis könnte auftreten, ist aber unwahrscheinlich	1 in 5-10 Jahren
3 - Möglich	Ereignis könnte auftreten	1 in 1-5 Jahren
4 - Wahrscheinlich	Ereignis wird wahrscheinlich auftreten	1-5 mal pro Jahr

Stufe	Beschreibung	Häufigkeit
5 - Sehr wahrscheinlich	Ereignis wird mit hoher Sicherheit auftreten	> 5 mal pro Jahr

### Auswirkung (Impact):

Stufe	Beschreibung	Finanzieller Schaden	Reputationsschaden	Compliance
1 - Vernachlässigbar	Minimale Auswirkung	< 10.000 €	Keine	Keine
2 - Gering	Geringe Auswirkung	10.000 - 50.000 €	Lokal	Kleinere Verstöße
3 - Mittel	Moderate Auswirkung	50.000 - 250.000 €	Regional	Meldepflichtige Vorfälle
4 - Hoch	Erhebliche Auswirkung	250.000 - 1 Mio. €	National	Bußgelder
5 - Sehr hoch	Katastrophale Auswirkung	> 1 Mio. €	International	Geschäftsverbot

### Risikomatrix:

Impact ↑						
5	M	H	H	VH	VH	
4	M	M	H	H	VH	
3	L	M	M	H	H	
2	L	L	M	M	H	
1	VL	L	L	M	M	
			→ Likelihood			
1	2	3	4	5		

### Legende:

VL = Very Low (Sehr niedrig)  
 L = Low (Niedrig)  
 M = Medium (Mittel)  
 H = High (Hoch)  
 VH = Very High (Sehr hoch)

### Risikoscore-Berechnung:

$$\text{Risikoscore} = \text{Wahrscheinlichkeit} \times \text{Auswirkung}$$

### Beispiel:

Wahrscheinlichkeit = 4 (Wahrscheinlich)

Auswirkung = 3 (Mittel)

Risikoscore =  $4 \times 3 = 12$  (Hoch)

### **7.3.4 3.4 Risiko-Eigentümer (Risk Owner)**

**Verantwortlichkeiten:** - Jedes identifizierte Risiko hat einen Risiko-Eigentümer - Risiko-Eigentümer ist verantwortlich für Risikobehandlung - Typischerweise: Asset Owner, Process Owner, oder CISO

**Eskalation:** - Hohe und sehr hohe Risiken werden an Geschäftsführung eskaliert - Siehe 0070\_ISMS\_Risikoakzeptanzkriterien.md

## **7.4 4. Quellen für Risikoinformationen**

### **7.4.1 4.1 Threat Intelligence**

**Externe Quellen:** - **CERT-Bund:** <https://www.cert-bund.de/> - **MITRE ATT&CK:** <https://attack.mitre.org/> - **NIST NVD:** <https://nvd.nist.gov/> - **Vendor Security Advisories:** Microsoft, Cisco, etc. - **Threat Intelligence Feeds:** [TODO: Kommerzielle Feeds]

**Interne Quellen:** - Security Incidents und Lessons Learned - Penetration Test Reports - Red Team Exercises

### **7.4.2 4.2 Schwachstellen (Vulnerabilities)**

**Vulnerability Scanning:** - **Tools:** [TODO: Nessus, Qualys, OpenVAS] - **Frequenz:** Wöchentlich (automatisiert) - **Scope:** Alle Systeme im ISMS-Scope

**CVE und CVSS:** - Common Vulnerabilities and Exposures (CVE) - Common Vulnerability Scoring System (CVSS) - Priorisierung nach CVSS-Score

**Patch Management:** - Siehe 0340\_Policy\_Vulnerability\_und\_Patch\_Management.md

### **7.4.3 4.3 Incidents und Findings**

**Security Incidents:** - Jeder Incident wird auf Risikorelevanz geprüft - Lessons Learned fließen in Risikoanalyse ein - Siehe 0400\_Policy\_Incident\_Management.md

**Audit-Findings:** - Interne und externe Audit-Findings - Findings werden als Risiken bewertet - Siehe 0130\_ISMS\_Internes\_Auditprogramm.md

## **7.5 5. Outputs des Risikomanagements**

### **7.5.1 5.1 Risikoregister**

**Inhalt:** - Alle identifizierten Risiken - Risikobewertung (Wahrscheinlichkeit, Auswirkung, Score) - Risiko-Eigentümer - Risikobehandlungsstrategie - Status und Maßnahmen

**Dokument:** 0080\_ISMS\_Risikoregister\_Template.md

**Pflege:** - Quartalsweise Review - Anlassbezogene Updates (neue Bedrohungen, Incidents)

### **7.5.2 5.2 Risikobehandlungsplan (Risk Treatment Plan)**

**Inhalt:** - Geplante Maßnahmen zur Risikobehandlung - Verantwortliche und Termine - Budget und Ressourcen - Priorisierung

**Dokument:** 0090\_ISMS\_Risikobehandlungsplan\_RTP\_Template.md

**Tracking:** - Maßnahmen werden im RTP getrackt - Regelmäßiges Reporting an CISO und Geschäftsführung

### 7.5.3 5.3 Statement of Applicability (SoA)

**Inhalt:** - Auswahl und Begründung von Annex A Controls - Basierend auf Risikoanalyse und Compliance-Anforderungen - Dokumentation von Ausschlüssen

**Dokument:** 0100\_ISMS\_Statement\_of\_Applicability\_SoA\_Template.md

**Zusammenhang:** - Risikoanalyse → Identifikation benötigter Controls - SoA → Dokumentation der Control-Auswahl - RTP → Implementierung der Controls

## 7.6 6. Risikomanagement-Zyklus

### 7.6.1 6.1 Regelmäßiger Review

**Frequenz:** - Quartalsweise: Review des Risikoregisters - **Jährlich:** Vollständige Risikoanalyse - **Anlassbezogen:** Bei wesentlichen Änderungen

**Trigger für anlassbezogenen Review:** - Neue Bedrohungen (z.B. Zero-Day-Exploits) - Wesentliche organisatorische Änderungen - Neue Compliance-Anforderungen - Major Security Incidents - Audit-Findings

### 7.6.2 6.2 Risikoüberwachung (Risk Monitoring)

**Kontinuierliches Monitoring:** - Security Monitoring (SIEM, IDS/IPS) - Vulnerability Scanning - Threat Intelligence Feeds - Incident Tracking

**KPIs:** - Anzahl offener Risiken (nach Risikostufe) - Durchschnittliche Zeit zur Risikobehebung - Anzahl akzeptierter Risiken - Trend der Risikoscores

**Reporting:** - Quartalsweise an Informationssicherheitsgremium - Jährlich im Management Review

### 7.6.3 6.3 Kontinuierliche Verbesserung

**Lessons Learned:** - Aus Security Incidents - Aus Audit-Findings - Aus Penetration Tests

**Verbesserungsmaßnahmen:** - Anpassung der Risikobewertungsskalen - Verbesserung der Risikoidentifikationsmethoden - Optimierung des Risikomanagement-Prozesses

## 7.7 7. Rollen und Verantwortlichkeiten

### 7.7.1 7.1 RACI-Matrix: Risikomanagement

Aktivität	CISO	ISMS Manager	Risk Owner	IT-Betrieb	Geschäftsführung
Risikomanagemen t/A Methodik definieren	R/IA	C	C	C	I

Aktivität	CISO	ISMS Manager	Risk Owner	IT-Betrieb	Geschäftsführung
Risikoidentifikation	R		C	C	I
Risikobewertung	R		C	C	I
Risikobehandlung	C		R	C	I
planen					
Maßnahmen	A	C	R	R	I
umsetzen					
Risikoakzeptanz	I		C	I	I
(niedrig/mittel)					
Risikoakzeptanz	I		C	I	A
(hoch/sehr hoch)					
Risikoüberwachung	R	R	C	C	I
Risiko- Reporting	R		C	I	I

**Legende:** R = Responsible, A = Accountable, C = Consulted, I = Informed

## 7.8 8. Referenzen

### 7.8.1 Interne Dokumente

- 0020\_ISMS\_Geltungsbereich\_Scope.md - ISMS Scope
- 0040\_ISMS\_Governance\_Rollen\_und\_Verantwortlichkeiten.md - Governance
- 0070\_ISMS\_Risikoakzeptanzkriterien.md - Risk Acceptance Criteria
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register
- 0090\_ISMS\_Risikobehandlungsplan\_RTP\_Template.md - Risk Treatment Plan
- 0100\_ISMS\_Statement\_of\_Applicability\_SoA\_Template.md - SoA
- 0340\_Policy\_Vulnerability\_und\_Patch\_Management.md - Vulnerability Management
- 0400\_Policy\_Incident\_Management.md - Incident Management

### 7.8.2 Externe Standards

- ISO/IEC 27001:2022 - Clause 6.1.2: Information security risk assessment
- ISO/IEC 27001:2022 - Clause 6.1.3: Information security risk treatment
- ISO/IEC 27005:2022 - Information security risk management
- NIST SP 800-30 - Guide for Conducting Risk Assessments

---

#### Genehmigt durch:

Thomas Weber, CISO

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

Nächster Review: {{ meta.document.next\_review }}

ewpage

# Chapter 8

## Risikokriterien und Risikoakzeptanz

**Dokument-ID:** 0070

**Dokumenttyp:** ISMS-Grundlagendokument

**Standard-Referenz:** ISO/IEC 27001:2022 Clause 6.1.2

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 8.1 1. Risikoappetit und Toleranz

#### 8.1.1 1.1 Risikoappetit

Die AdminSend GmbH definiert ihren Risikoappetit wie folgt:

**Allgemeiner Risikoappetit:** [TODO: Konservativ / Moderat / Progressiv]

Toleranzschwellen nach Risikostufe:

Risikostufe	Risikoscore	Akzeptabel	Behandlung erforderlich
Sehr niedrig	1-2	Ja	Monitoring
Niedrig	3-6	Ja	Monitoring
Mittel	7-12	Bedingt	Risikobehandlung empfohlen
Hoch	13-20	Nein	Risikobehandlung erforderlich
Sehr hoch	21-25	Nein	Sofortige Risikobehandlung

#### 8.1.2 1.2 Akzeptanzkriterien

**Automatisch akzeptabel:** - Risikoscore < 6 (Niedrig) - Keine Compliance-Verstöße - Keine kritischen Assets betroffen

**Bedingt akzeptabel:** - Risikoscore 7-12 (Mittel) - Mit Kompensationsmaßnahmen - Zeitlich befristet (max. 12 Monate)

**Nicht akzeptabel:** - Risikoscore 13 (Hoch/Sehr hoch) - Compliance-Verstöße - Kritische Assets ohne Schutzmaßnahmen

## 8.2 2. Bewertungsdimensionen

### 8.2.1 2.1 CIA-Triade

**Vertraulichkeit (Confidentiality):** - Schutz vor unbefugter Offenlegung - Klassifizierung: Öffentlich, Intern, Vertraulich, Streng vertraulich

**Integrität (Integrity):** - Schutz vor unbefugter Änderung - Korrektheit und Vollständigkeit von Informationen

**Verfügbarkeit (Availability):** - Sicherstellung des Zugriffs bei Bedarf - RTO/RPO-Anforderungen

### 8.2.2 2.2 Weitere Dimensionen

**Recht und Regulatorik:** - DSGVO-Compliance - Branchenspezifische Regulierung - Vertragliche Verpflichtungen

**Reputation:** - Auswirkungen auf Unternehmensimage - Kundenvertrauen - Medienberichterstattung

## 8.3 3. Akzeptanzprozess

### 8.3.1 3.1 Akzeptanzbefugnisse

Risikostufe	Akzeptanz durch	Dokumentation	Genehmigung
Sehr niedrig / Niedrig	CISO	Risikoregister	CISO
Mittel	CISO	Risikoregister + Begründung	CISO + CIO
Hoch	Geschäftsführung	Risikoregister + Formale Risikoakzeptanz	Geschäftsführung
Sehr hoch	Geschäftsführung	Risikoregister + Formale Risikoakzeptanz + Maßnahmenplan	Geschäftsführung

### 8.3.2 3.2 Dokumentationspflicht

**Mindestangaben:** - Risiko-ID und Beschreibung - Risikobewertung (Wahrscheinlichkeit, Auswirkung, Score) - Begründung für Akzeptanz - Kompensationsmaßnahmen (falls vorhanden) - Akzeptanzdatum und Gültigkeitsdauer - Akzeptierende Person

**Dokument:** Siehe 0080\_ISMS\_Risikoregister\_Template.md

### 8.3.3 3.3 Laufzeit von Akzeptanzen

**Befristung:** - Niedrige Risiken: Unbefristet (mit jährlichem Review) - Mittlere Risiken: Max. 12 Monate - Hohe Risiken: Max. 6 Monate - Sehr hohe Risiken: Max. 3 Monate (Ausnahme)

**Verlängerung:** - Erfordert erneute Bewertung und Genehmigung - Begründung für Verlängerung erforderlich

### 8.3.4 3.4 Review von akzeptierten Risiken

**Regelmäßiger Review:** - Quartalsweise: Alle akzeptierten Risiken - Jährlich: Vollständige Neubewertung

**Trigger für außerplanmäßigen Review:** - Neue Bedrohungen oder Schwachstellen - Änderung der Geschäftsumgebung - Security Incidents - Audit-Findings

## 8.4 4. Referenzen

### 8.4.1 Interne Dokumente

- 0060\_ISMS\_Risikomanagement\_Methodik.md - Risk Management Methodology
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register
- 0090\_ISMS\_Risikobehandlungsplan\_RTP\_Template.md - Risk Treatment Plan

### 8.4.2 Externe Standards

- ISO/IEC 27001:2022 - Clause 6.1.2: Information security risk assessment
- ISO/IEC 27005:2022 - Information security risk management

---

#### Genehmigt durch:

{{{ meta.management.ceo }}}, Geschäftsführung  
Datum: {{{ meta.document.approval\_date }}}

**Nächster Review:** {{{ meta.document.next\_review }}}

ewpage

# Chapter 9

## Risikoregister (Template)

**Dokument-ID:** 0080

**Dokumenttyp:** ISMS-Register/Template

**Standard-Referenz:** ISO/IEC 27001:2022 Clause 6.1.2

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Vertraulich

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 9.1 1. Zweck und Anleitung

#### 9.1.1 1.1 Zweck

Das Risikoregister dokumentiert alle identifizierten Informationssicherheitsrisiken im ISMS-Scope der **AdminSend GmbH**. Es dient als: - Zentrale Übersicht aller Risiken - Grundlage für Risikobehandlungssentscheidungen - Nachweis für Audits und Compliance - Basis für Risiko-Reporting

#### 9.1.2 1.2 Anleitung zur Verwendung

**Jede Zeile beschreibt ein Risiko:** - Eindeutige Risiko-ID (R-001, R-002, etc.) - Betroffenes Asset oder Prozess - Bedrohung und Schwachstelle - Risikobewertung (Wahrscheinlichkeit, Auswirkung, Score) - Risiko-Eigentümer - Behandlungsstrategie - Verknüpfung zu Controls und Maßnahmen

**Pflege:** - Quartalsweise Review durch ISMS Manager - Anlassbezogene Updates bei neuen Risiken - Archivierung behandelter/geschlossener Risiken

**Verknüpfungen:** - Controls: Siehe 0100\_ISMS\_Statement\_of\_Applicability\_SoA\_Template.md  
- Maßnahmen: Siehe 0090\_ISMS\_Risikobehandlungsplan\_RTP\_Template.md - Evidence: Siehe 0700\_Anhang\_Nachweisregister\_Evidence.md

## 9.2 2. Risikoregister-Tabelle

### 9.2.1 2.1 Aktive Risiken

Risiko-ID	Asset/Prozess	Beschreibung	Auswirkung	Wahrscheinlichkeit	Risiko-Score	Eigentümer	Behandlung	Mitgliedschaft	Status/Gitter	Termin	Bemerkungen
R-001	Netzwerkbox	Hardwareausfall bei device.config.switch.name	Kritische Schwäche	Mittel (3)	12	Mittel Anna Schmidt	Minderung	Redundanz	Offen	2026-06-30	Budget genehmigt
R-002	(DS-GVO)	Kunden-Datenschutzverletzung durch Back-ups	Hohes Risiko	Unzureichende Schutzmaßnahmen	20	Hoch Thomas Weber	Minderung	Immunität	Offen	2026-03-31	Siehe M-002
R-003	E-Mail-System	Phishingangriffe auf MFA-Nutzer	Hoch	Geringe Wahrscheinlichkeit	4	16	Hoch Anna Schmidt	Minderung	MFA für alle Benutzer	In Arbeit seit 28.02.2026	80% abgeschlossen
R-004	Entwicklungsabteilung	Suche nach Kryptographie in Secret-Code Scanning	Mittel	Hohe Wahrscheinlichkeit	3	9	Mittel Dev-Lead	Minderung	Secret-Scanning Tool	Geplant 2026-04-30	Tool-Evaluierung läuft
R-005	Remote-Zugriff	Unbefugter Zugriff auf VPN-Konfiguration	Unbekannt	Schwache Sicherheit	2	8	Mittel IT-Betrieb	Minderung	VPN-Hardening	Offen	2026-05-31

[TODO: Weitere Risiken hinzufügen basierend auf Risikoanalyse]

### 9.2.2 2.2 Akzeptierte Risiken

Risiko-ID	Asset/Prozess	Beschreibung	Risiko-Score	Eigentümer	Akzeptiert durch	Gültig bis	Review-Status		
R-010	Legacy-XYZ System	Ungepatched Systeme stellen Auslauf	System Schwach	Mittel (9)	Anna Schmidt	Thomas Weber	2026-01-15	2026-06-30	System wird am 30.06.2026 außer Betrieb genommen

Risiko-ID	Asset/Prozess	Fehlende Sicherheit	Risikostufe	Eigentümer	Akzeptiert	Gültig bis	Begründung	Review-Status
R-011	Testumgebung	Keine Verunsicherung	6	Niedrig Dev-Lead	Thomas Weber	2026-01-20	2027-01-20	Testumgebung nur synthetische Daten

[TODO: Akzeptierte Risiken dokumentieren]

### 9.2.3 2.3 Geschlossene/Behandelte Risiken (Archiv)

Risiko-ID	Asset/Prozess	Bedrohung	Score	Behandlung	Abschlussdatum	Bemerkungen
R-020	Webserver	Ungepatchte Schwachstelle	15	Mindern	2026-01-10	Patch installiert, Vulnerability Scan bestätigt
R-021	Firewall	CVE-2025-1234	Fehlkonfigurationen	Mindern	2026-01-15	Konfiguration korrigiert, Audit durchgeführt

[TODO: Geschlossene Risiken archivieren]

## 9.3 3. Risikokategorien und Klassifizierung

### 9.3.1 3.1 Risikokategorien

**Technische Risiken:** - Infrastruktur (Hardware, Netzwerk, Cloud) - Anwendungen (Software, Entwicklung) - Daten (Datenbanken, Backups, Verschlüsselung)

**Organisatorische Risiken:** - Prozesse (Fehlende oder unzureichende Prozesse) - Personal (Fehlende Kompetenzen, Insider-Bedrohung) - Lieferanten (Third-Party-Risiken)

**Physische Risiken:** - Standorte (Zutritt, Umweltrisiken) - Hardware (Diebstahl, Zerstörung)

**Compliance-Risiken:** - Regulatorische Anforderungen (DSGVO, NIS2, etc.) - Vertragliche Verpflichtungen

### 9.3.2 3.2 Bedrohungsquellen

**Externe Bedrohungen:** - Cyberkriminelle (Ransomware, Phishing, DDoS) - Hacktivisten - Nationalstaaten (APT) - Wettbewerber

**Interne Bedrohungen:** - Insider (böswillig oder fahrlässig) - Menschliche Fehler - Prozessfehler

**Umweltbedrohungen:** - Naturkatastrophen (Feuer, Wasser, Sturm) - Infrastrukturausfälle (Strom, Kühlung)

## 9.4 4. Risikobewertung

### 9.4.1 4.1 Bewertungsskalen

**Wahrscheinlichkeit (Likelihood):**

Stufe	Beschreibung	Häufigkeit
1	Sehr unwahrscheinlich	< 1 in 10 Jahren
2	Unwahrscheinlich	1 in 5-10 Jahren
3	Möglich	1 in 1-5 Jahren
4	Wahrscheinlich	1-5 mal pro Jahr
5	Sehr wahrscheinlich	> 5 mal pro Jahr

**Auswirkung (Impact):**

Stufe	Beschreibung	Finanziell	Reputation	Compliance
1	Vernachlässigbar	< 10k €	Keine	Keine
2	Gering	10-50k €	Lokal	Kleinere Verstöße
3	Mittel	50-250k €	Regional	Meldepflichtig
4	Hoch	250k-1M €	National	Bußgelder
5	Sehr hoch	> 1M €	International	Geschäftsverbot

**Risikoscore:** Wahrscheinlichkeit × Auswirkung

**Risikostufen:**

Score	Risikostufe	Farbe	Behandlung
1-2	Sehr niedrig	Grün	Monitoring
3-6	Niedrig	Grün	Monitoring
7-12	Mittel	Gelb	Behandlung empfohlen
13-20	Hoch	Orange	Behandlung erforderlich
21-25	Sehr hoch	Rot	Sofortige Behandlung

### 9.4.2 4.2 Behandlungsstrategien

**Vermeiden (Avoid):** - Aktivität einstellen, die das Risiko verursacht - Beispiel: Verzicht auf risikoreiche Technologie

**Mindern (Mitigate):** - Maßnahmen zur Reduzierung von Wahrscheinlichkeit oder Auswirkung - Beispiel: Implementierung von Controls (Firewall, MFA, Verschlüsselung)

**Übertragen (Transfer):** - Risiko auf Dritte übertragen - Beispiel: Cyber-Versicherung, Outsourcing mit SLA

**Akzeptieren (Accept):** - Bewusste Entscheidung, Risiko zu tragen - Nur für niedrige/mittlere Risiken nach Genehmigung - Siehe 0070\_ISMS\_Risikoakzeptanzkriterien.md

## 9.5 5. Risiko-Eigentümer und Verantwortlichkeiten

### 9.5.1 5.1 Risiko-Eigentümer (Risk Owner)

**Verantwortlichkeiten:** - Verantwortlich für Risikobehandlung - Entscheidung über Behandlungsstrategie - Überwachung der Maßnahmenumsetzung - Regelmäßige Risikobewertung

**Typische Risiko-Eigentümer:** - **CISO:** Übergreifende Sicherheitsrisiken - **CIO:** IT-Infrastruktur-Risiken - **Asset Owner:** Asset-spezifische Risiken - **Process Owner:** Prozessspezifische Risiken

### 9.5.2 5.2 RACI-Matrix: Risikomanagement

Aktivität	CISO	ISMS Manager	Risk Owner	IT-Betrieb
Risiko identifizieren	A	R	C	C
Risiko bewerten	A	R	C	C
Behandlung planen	A	C	R	C
Maßnahmen umsetzen	A	C	R	R
Risiko überwachen	A	R	C	C
Risikoregister pflegen	A	R	C	I

**Legende:** R = Responsible, A = Accountable, C = Consulted, I = Informed

## 9.6 6. Risiko-Reporting

### 9.6.1 6.1 Regelmäßiges Reporting

**Quartalsweise:** - Risiko-Dashboard an Informationssicherheitsgremium - Anzahl Risiken nach Stufe - Trend der Risikoscores - Status der Risikobehandlung

**Jährlich:** - Vollständiger Risikobericht im Management Review - Siehe 0140\_ISMS\_Management\_Review\_Template

### 9.6.2 6.2 Ad-hoc-Reporting

**Trigger:** - Neue kritische Risiken (Score > 13) - Wesentliche Änderung bestehender Risiken - Security Incidents mit Risikorelevanz

**Eskalation:** - Hohe Risiken: Sofortige Meldung an CISO und CIO - Sehr hohe Risiken: Sofortige Meldung an Geschäftsführung

## 9.7 7. Risiko-Review und Aktualisierung

### 9.7.1 7.1 Regelmäßiger Review

**Quartalsweise:** - Review aller aktiven Risiken - Aktualisierung von Bewertungen - Status-Update der Maßnahmen - Review akzeptierter Risiken

**Jährlich:** - Vollständige Risikoanalyse - Identifikation neuer Risiken - Archivierung geschlossener Risiken

### 9.7.2 7.2 Trigger für außerplanmäßigen Review

**Externe Trigger:** - Neue Bedrohungen (Zero-Day-Exploits, neue Malware) - Neue Schwachstellen (CVE-Veröffentlichungen) - Änderung der Bedrohungslage - Neue Compliance-Anforderungen

**Interne Trigger:** - Security Incidents - Audit-Findings - Wesentliche organisatorische Änderungen - Neue Assets oder Prozesse

## 9.8 8. Verknüpfungen und Referenzen

### 9.8.1 8.1 Verknüpfung zu anderen ISMS-Dokumenten

**Risikobehandlungsplan (RTP):** - Jedes Risiko mit Behandlung "Mindern" hat Maßnahmen im RTP - Siehe 0090\_ISMS\_Risikobehandlungsplan\_RTP\_Template.md

**Statement of Applicability (SoA):** - Controls im SoA sind basierend auf Risikoanalyse ausgewählt - Siehe 0100\_ISMS\_Statement\_of\_Applicability\_SoA\_Template.md

**Asset-Inventar:** - Risiken sind mit Assets verknüpft - Siehe 0720\_Anhang\_Asset\_und\_Systeminventar\_Template

**Incident Reports:** - Incidents können neue Risiken identifizieren - Siehe 0400\_Policy\_Incident\_Management.md

### 9.8.2 8.2 Interne Dokumente

- 0060\_ISMS\_Risikomanagement\_Methodik.md - Risk Management Methodology
- 0070\_ISMS\_Risikoakzeptanzkriterien.md - Risk Acceptance Criteria
- 0090\_ISMS\_Risikobehandlungsplan\_RTP\_Template.md - Risk Treatment Plan
- 0100\_ISMS\_Statement\_of\_Applicability\_SoA\_Template.md - SoA

### 9.8.3 8.3 Externe Standards

- ISO/IEC 27001:2022 - Clause 6.1.2: Information security risk assessment
- ISO/IEC 27005:2022 - Information security risk management
- NIST SP 800-30 - Guide for Conducting Risk Assessments

---

## 9.9 Änderungshistorie

Version	Datum	Autor	Beschreibung	Genehmigt durch
1.0	<pre>{{ meta.document.next_review }}</pre>	Thomas Weber	Initiale Version	<pre>{{ meta.management.ceo }}</pre>

---

**Genehmigt durch:**

Thomas Weber, CISO

Datum: 

```
{{ meta.document.approval_date }}
```

**Nächster Review:**

```
{{ meta.document.next_review }}
```

 (Quartalsweise)

ewpage

# Chapter 10

## Risikobehandlungsplan (RTP) – Template

**Dokument-ID:** 0090

**Dokumenttyp:** ISMS-Plan/Template

**Standard-Referenz:** ISO/IEC 27001:2022 Clause 6.1.3

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Vertraulich

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 10.1 1. Ziel und Geltungsbereich

#### 10.1.1 1.1 Ziel

Der Risikobehandlungsplan (Risk Treatment Plan, RTP) der **AdminSend GmbH** dokumentiert alle geplanten Maßnahmen zur Behandlung identifizierter Informationssicherheitsrisiken. Er dient als: - Aktionsplan für Risikobehandlung - Tracking-Tool für Maßnahmenumsetzung - Nachweis für Audits und Compliance - Basis für Ressourcenplanung und Budgetierung

#### 10.1.2 1.2 Geltungsbereich

Dieser Plan umfasst alle Maßnahmen zur Behandlung von Risiken im ISMS-Scope (siehe 0020\_ISMS\_Geltungsbereich\_Scope.md), die mit der Strategie “Mindern” oder “Übertragen” behandelt werden.

**Ausgeschlossen:** - Akzeptierte Risiken (siehe 0080\_ISMS\_Risikoregister\_Template.md) - Vermiedene Risiken (Aktivität eingestellt)

## 10.2 2. Risikobehandlungsplan-Tabelle

### 10.2.1 2.1 Aktive Maßnahmen

Maßnahm ID	Risiko- ID	Maßnah men-ID	Control- Referenz		Aufwand			Status	Fortschri tts	Bemerkungen
			Anex A)	Annex A)	Owner	Priorität(PT)	Budget	Zielterm		
M-001	R-001	Redundan t An 8.6		Anna Hoch	20	50.000	2026-06-30	Geplant	0%	Budget genehmigt, Ausschreibung läuft
M-002	R-002	Immutab ility An 8.13	Core (Capacity Switch management)	IT-Betrieb	Sehr hoch	40	30.000	2026-03-31	In Arbeit	60% Pilotphase abgeschlossen
M-003	R-003	MFA A.5.17 (Authentification für alle information)	(Autentication alle information)	IAM-Team	Sehr hoch	30	15.000	2026-02-28	In Arbeit	80% von 200 Be nutzern migriert
M-004	R-004	Secret-Scanning An 8.24 (Use of cryptogra phy Tool)	(Use of cryptogra phy Tool)	Dev-Lead	Mittel	15	10.000	2026-04-30	Geplant	10% Tool-Evaluierung: Git-Guardian vs. Gitleaks
M-005	R-005	VPN-Hardenin g An 5.14	(Information durch transfer) führen	IT-Betrieb	Mittel	10	5.000	2026-05-31	Geplant	0% Hardening-Guide erstellen

[TODO: Weitere Maßnahmen hinzufügen basierend auf Risikoregister]

### 10.2.2 2.2 Abgeschlossene Maßnahmen (Archiv)

Maßnahme-		Risiko-ID	Maßnahme	Owner	Abschlussdatum	Ergebnis	Nachweis/Evidence
ID							
M-010	R-020	Patch CVE- 2025- 1234 instal- lieren	IT- Betrieb		2026-01-10	Erfolgreich	Vulnerability Scan Report
M-011	R-021	Firewall- Konfiguration kor- rigieren	IT- Betrieb		2026-01-15	Erfolgreich	Firewall Audit Report

[TODO: Abgeschlossene Maßnahmen archivieren]

## 10.3 3. Maßnahmenpriorisierung

### 10.3.1 3.1 Priorisierungskriterien

**Prioritätsstufen:**

Priorität	Risikostufe	Compliance	Aufwand	Zeitrahmen
<b>Sehr hoch</b>	Sehr hoch / Hoch	Kritisch	Egal	Sofort - 3 Monate
<b>Hoch</b>	Hoch / Mittel	Wichtig	Niedrig- Mittel	3-6 Monate
<b>Mittel</b>	Mittel	Normal	Mittel	6-12 Monate
<b>Niedrig</b>	Niedrig	Optional	Hoch	> 12 Monate

**Priorisierungsformel:**

$$\text{Priorität} = (\text{Risikoscore} \times 2) + \text{Compliance-Faktor} - \text{Aufwand-Faktor}$$

**Compliance-Faktor:**

- Kritisch (DSGVO, NIS2): +10
- Wichtig (ISO 27001): +5
- Normal: +0

**Aufwand-Faktor:**

- Niedrig (< 10 PT): -0
- Mittel (10-40 PT): -5
- Hoch (> 40 PT): -10

### 10.3.2 3.2 Quick Wins

**Quick Wins** sind Maßnahmen mit hohem Nutzen und niedrigem Aufwand:

Maßnahme-ID	Maßnahme	Risikoreduktion	Aufwand	ROI
M-003	MFA-Rollout	Hoch	Mittel	Hoch
M-005	VPN-Hardening	Mittel	Niedrig	Sehr hoch

**Empfehlung:** Quick Wins sollten priorisiert werden, um schnelle Sicherheitsverbesserungen zu erzielen.

## 10.4 4. Maßnahmendetails

### 10.4.1 4.1 Maßnahmenbeschreibung

Für jede Maßnahme sollten folgende Details dokumentiert werden:

#### Maßnahme M-002: Immutable Backups implementieren

**Beschreibung:** Implementierung von unveränderlichen (immutable) Backups zum Schutz vor Ransomware. Backups werden in einem Write-Once-Read-Many (WORM) Format gespeichert und können nicht gelöscht oder modifiziert werden.

**Ziel:** - Schutz vor Ransomware-Angriffen auf Backups - Sicherstellung der Wiederherstellbarkeit bei Datenverlust - Compliance mit DSGVO Art. 32 (Sicherheit der Verarbeitung)

**Scope:** - Alle produktiven Systeme - Kritische Datenbanken - Kundendaten (DSGVO-relevant)

**Implementierungsschritte:** 1. Backup-Lösung evaluieren (Veeam, Commvault, AWS S3 Object Lock) 2. Pilotphase mit nicht-kritischen Systemen ( Abgeschlossen) 3. Rollout auf produktive Systeme (In Arbeit) 4. Restore-Tests durchführen 5. Dokumentation und Schulung

**Ressourcen:** - Owner: IT-Betrieb - Team: 2 Backup-Administratoren - Aufwand: 40 Personentage - Budget: 30.000 € (Lizenzen + Hardware)

**Abhängigkeiten:** - Keine kritischen Abhängigkeiten

**Risiken der Umsetzung:** - Erhöhter Speicherbedarf (Mitigation: Zusätzlicher Storage beschafft) - Längere Backup-Zeiten (Mitigation: Backup-Fenster angepasst)

**Erfolgskriterien:** - Alle kritischen Systeme haben immutable Backups - Restore-Tests erfolgreich (RTO/RPO eingehalten) - Keine Ransomware kann Backups löschen

**Nachweis/Evidence:** - Backup-Konfigurationsdokumentation - Restore-Test-Protokolle - Compliance-Bericht

## 10.5 5. Control-Mapping (Annex A)

### 10.5.1 5.1 Verknüpfung zu Annex A Controls

Jede Maßnahme sollte mit relevanten Annex A Controls verknüpft werden:

Maßnahme-ID	Annex A Control	Control-Name	Implementierungsstatus
M-001	A.8.6	Capacity management	Geplant

Maßnahme-ID	Annex A Control	Control-Name	Implementierungsstatus
M-002	A.8.13	Information backup	In Arbeit
M-003	A.5.17	Authentication information	In Arbeit
M-004	A.8.24	Use of cryptography	Geplant
M-005	A.5.14	Information transfer	Geplant

**Vollständiges Control-Mapping:** - Siehe 0100\_ISMS\_Statement\_of\_Applicability\_SoA\_Template.md  
- Siehe 0710\_Anhang\_AnnexA\_Mapping\_Template.md

## 10.5.2 5.2 Control-Implementierungsstatus

### Status-Definitionen:

Status	Beschreibung	Kriterien
<b>Nicht implementiert</b>	Control ist nicht vorhanden	0% Umsetzung
<b>Geplant</b>	Control ist geplant, aber noch nicht begonnen	Maßnahme im RTP
<b>In Arbeit</b>	Control wird gerade implementiert	1-99% Umsetzung
<b>Implementiert</b>	Control ist vollständig implementiert	100% Umsetzung, Evidence vorhanden
<b>Wirksam</b>	Control ist implementiert und nachweislich wirksam	Implementiert + Wirksamkeitsnachweis

## 10.6 6. Ressourcenplanung und Budgetierung

### 10.6.1 6.1 Ressourcenübersicht

#### Personelle Ressourcen:

Team/Rolle	Verfügbare Kapazität (PT/Monat)	Geplante Auslastung	Verfügbarkeit
IT-Betrieb	40	30	75%
Security Team	20	18	90%
IAM-Team	15	12	80%
Dev-Team	10	5	50%

#### Finanzielle Ressourcen:

Quartal	Budget	Geplante Ausgaben	Verfügbar
Q1 2026	50.000 €	45.000 €	5.000 €
Q2 2026	50.000 €	55.000 €	-5.000 € (Überziehung)
Q3 2026	50.000 €	30.000 €	20.000 €
Q4 2026	50.000 €	20.000 €	30.000 €

**Budgetanforderung:** - Q2 2026: Zusätzliche 5.000 € für M-001 (Redundanter Switch)

## 10.6.2 6.2 Kapazitätsplanung

**Engpässe:** - Security Team: 90% ausgelastet (kritisch) - IAM-Team: 80% ausgelastet (hoch)

**Maßnahmen:** - Priorisierung kritischer Maßnahmen - Externe Unterstützung für M-004 (Secret-Scanning) - Verschiebung nicht-kritischer Maßnahmen auf Q3/Q4

## 10.7 7. Abhängigkeiten und Risiken der Umsetzung

### 10.7.1 7.1 Abhängigkeiten zwischen Maßnahmen

M-002 (Immutable Backups)

↓ (benötigt)

M-001 (Redundanter Switch)

↓ (ermöglicht)

M-005 (VPN-Hardening)

**Kritischer Pfad:** - M-002 muss vor M-001 abgeschlossen sein - M-001 ist Voraussetzung für M-005

### 10.7.2 7.2 Risiken der Umsetzung

Risiko	Wahrscheinlichkeit	Auswirkung	Mitigation
Ressourcenengpässen	Hoch	Mittel	Externe Unterstützung, Priorisierung
Budgetüberschreitung	Mittel	Mittel	Regelmäßiges Budget-Monitoring, Genehmigungsprozess
Technische Komplexität	Mittel	Hoch	Pilotphasen, externe Expertise
Widerstand gegen Änderungen	Niedrig	Mittel	Change Management, Awareness

### 10.7.3 7.3 Change Management

**Kommunikation:** - Regelmäßige Updates an Stakeholder - Awareness-Kampagnen für betroffene Benutzer - Schulungen für neue Controls

**Rollback-Planung:** - Für jede Maßnahme Rollback-Plan erstellen - Pilotphasen vor Produktiv-Rollout - Backup vor kritischen Änderungen

## 10.8 8. Tracking und Reporting

### 10.8.1 8.1 Maßnahmen-Tracking

**Tracking-Frequenz:** - Wöchentlich: Status-Update für kritische Maßnahmen - Monatlich: Vollständiges RTP-Review - Quartalsweise: Reporting an Informationssicherheitsgremium

**Tracking-Metriken:** - Anzahl offener Maßnahmen - Anzahl überfälliger Maßnahmen - Durchschnittliche Umsetzungsdauer - Budget-Auslastung

### 10.8.2 8.2 Reporting

**Monatliches Reporting:** - Status aller aktiven Maßnahmen - Fortschritt (% Completion) - Risiken und Probleme - Budget-Status

**Quartalsweises Reporting:** - Zusammenfassung für Informationssicherheitsgremium - Trend-Analyse - Priorisierungsempfehlungen

**Eskalation:** - Überfällige Maßnahmen (> 2 Wochen): Eskalation an CISO - Kritische Verzögerungen: Eskalation an Geschäftsführung

## 10.9 9. Wirksamkeitsprüfung

### 10.9.1 9.1 Nachweis der Wirksamkeit

Für jede implementierte Maßnahme muss die Wirksamkeit nachgewiesen werden:

**Nachweismethoden:** - **Technische Tests:** Vulnerability Scans, Penetration Tests, Configuration Audits - **Prozess-Audits:** Internal Audits, Compliance Checks - **Monitoring:** SIEM-Alerts, Log-Analyse, KPI-Tracking - **Dokumentation:** Policies, Procedures, Training Records

**Beispiel M-002 (Immutable Backups):** - Nachweis: Restore-Test-Protokoll - Frequenz: Quartalsweise - Kriterien: RTO/RPO eingehalten, Backups nicht modifizierbar

### 10.9.2 9.2 Evidence-Register

**Verknüpfung:** - Siehe 0700\_Anhang\_Nachweisregister\_Evidence.md - Jede Maßnahme hat verknüpfte Evidence

## 10.10 10. Rollen und Verantwortlichkeiten

### 10.10.1 10.1 RACI-Matrix: Risikobehandlung

Aktivität	CISO	ISMS Manager	Maßnahmen-Owner	IT-Betrieb	Budget-Owner
RTP erstellen	A	R	C	C	I

Aktivität	CISO	ISMS Manager	Maßnahmen-Owner	IT-Betrieb	Budget-Owner
Maßnahmen priorisieren	A	R	C	C	C
Maßnahmen umsetzen	A	C	R	R	I
Budget freigeben	C	I	I	I	A
Fortschritt tracken	A	R	C	I	I
Wirksamkeit prüfen	A	R	C	R	I
RTP-Review	A	R	C	C	I

**Legende:** R = Responsible, A = Accountable, C = Consulted, I = Informed

## 10.11 11. Referenzen

### 10.11.1 11.1 Interne Dokumente

- 0060\_ISMS\_Risikomanagement\_Methodik.md - Risk Management Methodology
- 0070\_ISMS\_Risikoakzeptanzkriterien.md - Risk Acceptance Criteria
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register
- 0100\_ISMS\_Statement\_of\_Applicability\_SoA\_Template.md - SoA
- 0360\_Policy\_Change\_und\_Release\_Management.md - Change Management
- 0700\_Anhang\_Nachweisregister\_Evidence.md - Evidence Register

### 10.11.2 11.2 Externe Standards

- ISO/IEC 27001:2022 - Clause 6.1.3: Information security risk treatment
- ISO/IEC 27002:2022 - Information security controls
- ISO/IEC 27005:2022 - Information security risk management

---

## 10.12 Änderungshistorie

Version	Datum	Autor	Beschreibung	Genehmigt durch
1.0	{{ meta.document.date}} {{ meta.document.approval_date}}	Thomas	Initiale Version	{{ meta.management.ceo}} {{ }}}

---

### Genehmigt durch:

Thomas Weber, CISO

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (Monatlich)

ewpage

# Chapter 11

## Statement of Applicability (SoA) – Template

**Dokument-ID:** 0100

**Dokumenttyp:** ISMS-Nachweis/Template

**Standard-Referenz:** ISO/IEC 27001:2022 Clause 6.1.3 d), Annex A

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Vertraulich

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 11.1 1. Zweck und Geltungsbereich

#### 11.1.1 1.1 Zweck

Das Statement of Applicability (SoA) der **AdminSend GmbH** dokumentiert: - Welche Annex A Controls auf das ISMS anwendbar sind - Begründung für die Auswahl oder Ausschluss von Controls - Implementierungsstatus jedes Controls - Verknüpfung zu Policies, Richtlinien und Evidence

Das SoA ist ein **Pflichtdokument** nach ISO/IEC 27001:2022 und dient als: - Nachweis der systematischen Control-Auswahl - Grundlage für Audits und Zertifizierungen - Übersicht über den Implementierungsstatus - Verknüpfung zwischen Risikoanalyse und Controls

#### 11.1.2 1.2 Geltungsbereich

Dieses SoA gilt für den gesamten ISMS-Scope (siehe 0020\_ISMS\_Geltungsbereich\_Scope.md): - Alle Standorte: {{ netbox.site.name }} und weitere - Alle IT-Systeme und Infrastruktur - Alle Geschäftsprozesse im Scope - Alle Informationswerte

### 11.1.3 1.3 Annex A Controls (ISO 27001:2022)

**ISO/IEC 27001:2022 Annex A** enthält 93 Controls in 4 Kategorien: - **Organisational Controls (5.x):** 37 Controls - **People Controls (6.x):** 8 Controls - **Physical Controls (7.x):** 14 Controls - **Technological Controls (8.x):** 34 Controls

**Amendment 1:2024:** - Berücksichtigt Änderungen aus Amendment 1:2024 - Siehe 0710\_Anhang\_AnnexA\_Mapping für vollständige Liste

## 11.2 2. Control-Auswahlkriterien

### 11.2.1 2.1 Auswahlprozess

Controls werden basierend auf folgenden Kriterien ausgewählt:

- 1. Risikoanalyse:** - Controls zur Behandlung identifizierter Risiken - Siehe 0080\_ISMS\_Risikoregister\_Template
- 2. Compliance-Anforderungen:** - Gesetzliche Anforderungen (DSGVO, NIS2, etc.) - Vertragliche Verpflichtungen - Branchenstandards
- 3. Best Practices:** - Branchenübliche Sicherheitsmaßnahmen - Empfehlungen von Sicherheitsexperten
- 4. Organisatorische Anforderungen:** - Geschäftsanforderungen - Stakeholder-Erwartungen

### 11.2.2 2.2 Ausschlusskriterien

Controls können ausgeschlossen werden, wenn: - Nicht relevant für den ISMS-Scope - Risiko ist akzeptiert und Control nicht erforderlich - Alternative Controls bieten gleichwertigen Schutz - Technisch oder organisatorisch nicht umsetzbar (mit Begründung)

**Wichtig:** Ausschlüsse müssen begründet werden und dürfen die Fähigkeit der Organisation zur Erfüllung von Sicherheitsanforderungen nicht beeinträchtigen.

## 11.3 3. Statement of Applicability (SoA) - Übersicht

### 11.3.1 3.1 Implementierungsstatus

Status	Anzahl Controls	Prozent
Implementiert	[TODO]	[TODO]%
In Arbeit	[TODO]	[TODO]%
Geplant	[TODO]	[TODO]%
Nicht anwendbar	[TODO]	[TODO]%
<b>Gesamt</b>	<b>93</b>	<b>100%</b>

**Ziel:** Mindestens 80% der anwendbaren Controls implementiert bis [TODO: Datum]

### 11.3.2 3.2 Implementierung nach Kategorie

Kategorie	Anwendbar	Implementiert	In Arbeit	Geplant	Nicht anwendbar
Organisational (5.x)	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
People (6.x)	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
Physical (7.x)	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
Technological (8.x)	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

## 11.4 4. SoA-Tabelle: Organisational Controls (5.x)

### 11.4.1 4.1 Policies for Information Security (5.1-5.10)

Control-Control-ID	Name	Anwendbar (Ja/Nein)	Begründung Implementierung/Herausstanzung/Beschriftung/richtige Einheiten	Bemerkungen	
				Herausstanzung/Beschriftung	richtige Einheiten
A.5.1	Policies for information security	Ja	- Implementiert ISMS-Leitlinie und themen-spezifische Policies	0010_ISMS_Policies_für_sicherheit	Dokument Webside Re-view
A.5.2	Information security roles and responsibilities	Ja	- Implementiert ISMS-Governance-Struktur definiert	0040_ISMS_Rollen_und_Verantw	Matrize Web
A.5.3	Segregation of duties	Ja	- In Arbeit Rollentrennung in kritischen Prozessen	0220_Policy_Aufgabenseparation	Aufgabenseparation Konfiguration gesetzt
A.5.4	Management responsibilities	Ja	- Implementiert Management Commitment dokumentiert	0010_ISMS_Managementsicherheitsleitlinie	Re-meta.management.ceo view } }
A.5.5	Contact with authorities	Ja	- Implementiert Kontakte zu Behörden dokumentiert	0050_Kontakt_mit_Behörden	Kontakt mit Behörden Dokumentation.md Web

Control-Control-ID	Name	Anwendung (Ja/ Nein)	Begründung	Implementierung	Hinweise		Own Bemerkungen
					Bestätigung	Policy	
A.5.6	Contact with special interest groups	Ja	-	Implementiert Mitgliedschaft [TODO: in CERT, Branchenverbänden]	Mitgliedschaft [TODO: Dokument]	Threats nachweise Weber	
A.5.7	Threat intelligence	Ja	-	In Arbeit	Threat Intelligence Feeds abonniert	0060_ISMS_Eisiko Management MIRE Methodik.md Feed- Team ATT&CK, KonfigurationCERT	
A.5.8	Information security in project management	Ja	-	Geplant	Security in Projektlebenszyklus	0680_Policy_ProjektPMQ_RollProjects.md Checklisten Q2 2026	
A.5.9	Inventory of information and other associated assets	Ja	-	In Arbeit	Asset-Inventar wird gepflegt	0720_Anhang_GMBET und 89% Systeminventar_Te Net- Betriebs- Box fasst	
A.5.10	Acceptable use of information and other associated assets	Ja	-	Implementiert Acceptable Use Policy	Acceptable Use Policy	0200_Policy_Signifikante_Nutzung_IT.md Policies	

[TODO: Vollständige Tabelle für alle 37 Organisational Controls erstellen]

## 11.5 5. SoA-Tabelle: People Controls (6.x)

Control-Control-ID	Name	Anwendung (Ja/Nein)	Begründung	Implementierung	Hinweise	Rechtsgrundlage	Own Bemerkungen
A.6.1	Screening	Ja	-	Implementiert Background Checks für kritische Rollen	0520_Policy_HR_Security.md	HR Security	
A.6.2	Terms and conditions of employment	Ja	-	Implementiert Sicherheitsklassen in Arbeitsverträgen	0530_Richtlinie_HR_Boarding_Rollenwechselfristen	HR Security	
A.6.3	Information security awareness, education and training	Ja	-	In Arbeit	Security Awareness Programm	0120_ISMS_Schulung_Theorie und Praxis	Theorie und Praxis wird Kompetenz übertragen
A.6.4	Disciplinary process	Ja	-	Implementiert Disziplinarverfahren bei Verstößen	0520n_Policy_HR_Security.md	HR Security	
A.6.5	Responsibilities after termination or change of employment	Ja	-	Implementiert Offboarding-Prozess	0530_Richtlinie_HR_Boarding_Rollenwechselfristen	Offboarding	Checkliste
A.6.6	Confidentiality or non-disclosure agreements	Ja	-	Implementiert NDAs für Mitarbeiter und Dritte	0520_Policy_SignRed_Security.md	SignRed Security	NDAs
A.6.7	Remote working	Ja	-	Implementiert Remote Work Policy	0500_Policy_Remote_Device_und_Remote_Work	Mobile Device und Remote Work	Schmidt Guide-lines

Control-Control-ID	Name	Anwendung (Ja/ Nein)	Begründung	Implementierung	Gesetz/Pol.	Richtlinien	Hinweise	Own	Bemerkungen
A.6.8	Information security event reporting	-		Implementiert Incident Reporting Prozess	0400_Policy_Incident_Management.md			Re- ports	We- ber

## 11.6 6. SoA-Tabelle: Physical Controls (7.x)

Control-Control-ID	Name	Anwendung (Ja/ Nein)	Begründung	Implementierung	Gesetz/Pol.	Richtlinien	Hinweise	Own	Bemerkungen
A.7.1	Physical security perimeter	-		Implementiert Zugrittskontrolle am Standort {{ net-box.site.name }}	0480_Policy_Physikalische_Sicherheit.md			Mgmt	
A.7.2	Physical entry	-		Implementiert Zugangskartenmanagement Besucher- management	0490_Richtlinie_Einfuehrung_Besucher_und_So			Mgmt	
A.7.3	Securing offices, rooms and facilities	-		Implementiert Serverraum gesichert, Alarmanlagen	0480_Policy_Physikalische_Sicherheit.md			Mgmt	
A.7.4	Physical monitoring	-		Implementiert Videoüberwachung Alarmsysteme	0480_Policy_Physikalische_Sicherheit.md			Mgmt	konform
A.7.5	Protecting against physical environmental men- tal threats	-		Implementiert Brandschutz, Klimatisierung, USV	0480_Policy_Physikalische_Sicherheit.md			Mgmt	

Control-Control-ID	Name	Anwendung (Ja/Nein)	Begründung	Implementierung	Urgenzstatus	Besitzstatus/Besitzvertrag	Rechtsgrundlage	Hinweise	Owner	Bemerkungen
A.7.6	Working in secure areas	Ja	-	Implementiert Clean Desk Policy, Secure Areas	Clean Desk Policy, Secure Areas	0480_Policy_Auf_Phys_Facility_Sicherheit.md	Auf Phys Facility Sicherheit	Sicherheit	Mgmt	Bericht
A.7.7	Clear desk and clear screen	Ja	-	In Arbeit Clear Desk Policy kommuniziert	Clear Desk Policy kommuniziert	0480_Policy_Auf_Phys_Theorie_Sicherheit.md	Auf Phys Theorie Sicherheit	Kampagne	Weber	läuft
A.7.8	Equipment siting and protection	Ja	-	Implementiert Equipment-Schutz, Diebstahlsicherung	Equipment-Schutz, Diebstahlsicherung	0490_Richtlinie_Eintritt_Besucher_und_So	Richtlinie Eintritt Besucher und So	Registrierung	Betrieb	
A.7.9	Security of assets off-premises	Ja	-	Implementiert Laptop-Verschlüsselung, Mobile Device Policy	Laptop-Verschlüsselung, Mobile Device Policy	0500_Policy_Mobile_Device_und_Remote_Wo	Mobile Device und Remote Work	Konfiguration	Betrieb	
A.7.10	Storage media	Ja	-	Implementiert Sichere Handhabung von Speichermedien	Sichere Handhabung von Speichermedien	0280_Policy_Handlung_Klassifizierung_und_In	Handlung Klassifizierung und Information	Procedere	Betrieb	
A.7.11	Supporting utilities	Ja	-	Implementiert USV, Notstrom, Klimatisierung	USV, Notstrom, Klimatisierung	0480_Policy_W_Phys_Facility_Sicherheit.md	W Phys Facility Sicherheit	Mgmt		
A.7.12	Cabling security	Ja	-	Implementiert Strukturierte Verkaubelung, Schutz	Strukturierte Verkaubelung, Schutz	0480_Policy_Verkauf_Empfang_Sicherheit.md	Verkauf Empfang Sicherheit	Betrieb		
A.7.13	Equipment maintenance	Ja	-	Implementiert Wartungsvertretung, Wartungsprotokolle	Wartungsvertretung, Wartungsprotokolle	0480_Policy_W_Phys_Facility_Sicherheit.md	W Phys Facility Sicherheit	Betrieb		
A.7.14	Secure disposal or re-use of equipment	Ja	-	Implementiert Sichere Entsorgung, Data Wiping	Sichere Entsorgung, Data Wiping	0580_Policy_E_Auslagerung_wiede_Loeschung.	E Auslagerung wieder Loeschung	Betriebskonform		

## 11.7 7. SoA-Tabelle: Technological Controls (8.x)

Control-ID	Control-Name	Anwendung (bei Nein)	Begründung	Implementierung	Urgenzstatus	Besitz/Besitz	Richtlinie	Hinweise	Owner	Bemerkungen
A.8.1	User endpoint devices	Ja	-	Implementiert Endpoint Protection (EDR/AV)	Endpunkt (EDR/AV)	0620_Policy_EndePnt_Security.md	EDR/AV Betrieb Konfiguration			
A.8.2	Privileged access rights	Ja	-	In Arbeit	PAM-Lösung wird implementiert	0220_Policy_PAMgriffsRechte_und_IdentSystemBetriebeQ2	PAMgriffsRechte_und_Ident SystemBetriebeQ2 2026			
A.8.3	Information access restriction	Ja	-	Implementiert Zugriffskontrolle RBAC	Zugriffskontrolle RBAC	1020_Policy_Authentifizierung_und_IdentKonfiguration	Aufzugriffssteuerung_und_Ident Konfiguration			
A.8.4	Access to source code	Ja	-	Implementiert Git-Zugriffskontrollen, Code Review	Git-Zugriffskontrollen, Code Review	0360_Policy_GitSecurityDevelopment.md	GitSecurityDevelopment.md			
A.8.5	Secure authentication	Ja	-	In Arbeit	MFA-Rollout	0240_Policy_MFAAuthentisierung_und_Passwoerde	MFAAuthentisierung_und_Passwoerde Konfiguration geschlossen			
A.8.6	Capacity management	Ja	-	In Arbeit	Monitoring, Kapazitätsplanung	[TODO: Policy]	Monitoring - Dashboard			
A.8.7	Protection against malware	Ja	-	Implementiert Antivirus, EDR, Email-Filtering	Antivirus, EDR, Email-Filtering	0620_Policy_Endpunkt_Security.md	Antivirus Betrieb Reports			
A.8.8	Management of technical vulnerabilities	Ja	-	In Arbeit	Vulnerability Management Prozess	0340_Policy_ScanVulnerability_und_Patch_Management	ScanVulnerability_und_Patch_Management Reports			

[TODO: Vollständige Tabelle für alle 34 Technological Controls erstellen]

## 11.8 8. Nicht anwendbare Controls

### 11.8.1 8.1 Ausgeschlossene Controls mit Begründung

Control-ID	Control-Name	Begründung für Ausschluss	Alternative Maßnahmen	Genehmigt durch
[TODO]	[TODO]	[TODO: Nicht im Scope, Risiko akzeptiert, etc.]	[TODO: Falls vorhanden]	Thomas Weber

**Wichtig:** Ausschlüsse müssen dokumentiert und genehmigt werden. Sie dürfen die Fähigkeit zur Erfüllung von Sicherheitsanforderungen nicht beeinträchtigen.

## 11.9 9. Verknüpfungen und Referenzen

### 11.9.1 9.1 Verknüpfung zu ISMS-Dokumenten

**Risikoanalyse:** - Controls sind basierend auf Risikoanalyse ausgewählt - Siehe 0080\_ISMS\_Risikoregister\_Template.md

**Risikobehandlungsplan:** - Implementierung von Controls ist im RTP getrackt - Siehe 0090\_ISMS\_Risikobehandlungsplan\_RTP\_Template.md

**Policies und Richtlinien:** - Jedes Control ist mit Policy/Richtlinie verknüpft - Siehe ISMS-Dokumentenstruktur (0200-0690)

**Evidence:** - Nachweise für Control-Implementierung - Siehe 0700\_Anhang\_Nachweisregister\_Evidence.md

### 11.9.2 9.2 Vollständiges Annex A Mapping

Für eine vollständige Übersicht aller 93 Annex A Controls siehe: - 0710\_Anhang\_AnnexA\_Mapping\_Template.md

## 11.10 10. Review und Aktualisierung

### 11.10.1 10.1 Regelmäßiger Review

**Jährlich:** - Vollständiger SoA-Review - Überprüfung der Anwendbarkeit aller Controls - Aktualisierung des Implementierungsstatus

**Quartalsweise:** - Review des Implementierungsstatus - Tracking der Maßnahmen aus RTP

### 11.10.2 10.2 Trigger für außerplanmäßigen Review

**Änderungen am ISMS-Scope:** - Neue Standorte, Systeme, Prozesse - Siehe 0020\_ISMS\_Geltungsbereich\_Scope.md

**Neue Risiken:** - Wesentliche Änderungen im Risikoregister - Siehe 0080\_ISMS\_Risikoregister\_Template.md

**Neue Compliance-Anforderungen:** - Neue Gesetze, Regulierungen, Verträge

**Audit-Findings:** - Interne oder externe Audit-Findings

## 11.11 11. Referenzen

### 11.11.1 11.1 Interne Dokumente

- 0020\_ISMS\_Geltungsbereich\_Scope.md - ISMS Scope
- 0060\_ISMS\_Risikomanagement\_Methodik.md - Risk Management

- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register
- 0090\_ISMS\_Risikobehandlungsplan\_RTP\_Template.md - Risk Treatment Plan
- 0710\_Anhang\_AnnexA\_Mapping\_Template.md - Complete Annex A Mapping
- Alle Policies (0200-0680) und Richtlinien (0210-0690)

## 11.11.2 11.2 Externe Standards

- ISO/IEC 27001:2022 - Clause 6.1.3 d): Statement of Applicability
  - ISO/IEC 27001:2022 - Annex A: Information security controls
  - ISO/IEC 27001:2022/Amd 1:2024 - Amendment 1 (Annex A updates)
  - ISO/IEC 27002:2022 - Information security controls (detailed guidance)
- 

## 11.12 Änderungshistorie

Version	Datum	Autor	Beschreibung	Genehmigt durch
1.0	{{ meta.document.Wdate }} 	Thomas	Initiale Version	{{ meta.management.ceo }} 

---

### Genehmigt durch:

Thomas Weber, CISO

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (Jährlich)

ewpage

# Chapter 12

## Informationssicherheitsziele und Metriken

**Dokument-ID:** 0110

**Dokumenttyp:** ISMS-Grundlagendokument

**Standard-Referenz:** ISO/IEC 27001:2022 Clause 6.2

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 12.1 1. Informationssicherheitsziele

#### 12.1.1 1.1 Strategische Ziele

Die AdminSend GmbH definiert folgende strategische Informationssicherheitsziele:

Ziel-ID	Ziel	Beschreibung	KPI/Metrik	Zielwert	Messmethode	Owner	Frequenz	Status
Z-001	Compliance	Inhaltung sich- er- stellen traglichen Anforderun- gen	Anzahl aller gesetzlichen Verstöße	0	Audit- Berichte, Incident Reports	Thomas Weber	Quartalsweiter	Aktiv
Z-002	Risiken Reduzierung	min- imieren sehr hoher Risiken	Anzahl Risiken mit Score	< 5 13	Risikoregister	Thomas Weber	Quartalsweiter	Aktiv

Ziel-ID	Ziel	Beschreibung	KPI/Metrik	Zielwert	Messmethode	Owner	Frequenz	Status
Z-003	Verfügbarkeit gewährleistung der Verfüg- ten barkeit kritischer Systeme	Sicher- stellungs- der Verfü- gbarkeit kritischer Systeme	Uptime kritischer Systeme	99,5%	Monitoring- System	Anna Schmidt	Monatlich	Aktiv
Z-004	Incident- reduzierung der Anzahl der Anzahl dutzierer Sicher- heitsvorfälle	Reduzierung der Anzahl der Anzahl dutzierer Sicher- heitsvorfälle	Anzahl Security Incidents	< 10 pro Quartal	Incident Manage- ment System	Thomas Weber	Quartalsweise	Aktiv
Z-005	Awaren- steigerung des Sicher- höhen heitsbe- wusstseins	Steigerung des Sicher- höhen heitsbe- wusstseins	Schulungsteil- nahme- Quote	100%	LMS, Schu- lungsna- chweise	Thomas Weber	Jährlich	Aktiv
Z-006	Patch- Compliance Installation kritischer Patches	Zeitnahe Installation Patch- Installation (kritisch)	Durchschnittliche Zeit zur Patch- Installation	7 Tage	Vulnerability Manage- ment System	IT- Betrieb	Monatlich	Aktiv

[TODO: Weitere organisationsspezifische Ziele hinzufügen]

### 12.1.2 1.2 Operative Ziele

Ziel-ID	Ziel	KPI/Metrik	Zielwert	Owner	Frequenz
Z-010	MFA- Rollout ab- schließen	MFA- Aktivierungsrate	100%	IT-Betrieb	Monatlich
Z-011	Vulnerability Management	Durchschnittliche Zeit zur Behebung hoher Schwachstellen	< 30 Tage	IT-Betrieb	Monatlich
Z-012	Backup- Tests	Erfolgsrate Restore-Tests	100%	IT-Betrieb	Quartalsweise
Z-013	Phishing- Resilienz	Phishing-Klickrate bei Simulationen	< 5%	Thomas Weber	Quartalsweise

## 12.2 2. Key Performance Indicators (KPIs)

### 12.2.1 2.1 Sicherheits-KPIs

**Risikomanagement:** - Anzahl identifizierter Risiken (nach Stufe) - Anzahl behandelter Risiken pro Quartal - Durchschnittliche Risikobehebungszeit - Anzahl akzeptierter Risiken

**Incident Management:** - Anzahl Security Incidents (nach Schweregrad) - Mean Time to Detect (MTTD) - Mean Time to Respond (MTTR) - Mean Time to Recover (MTTR)

**Vulnerability Management:** - Anzahl offener Schwachstellen (nach CVSS-Score) - Durchschnittliche Zeit zur Patch-Installation - Patch-Compliance-Rate

**Access Management:** - Anzahl privilegierter Accounts - MFA-Aktivierungsrate - Rezertifizierungsrate - Anzahl Zugriffsverletzungen

**Awareness und Training:** - Schulungsteilnahme-Quote - Phishing-Simulation-Ergebnisse - Anzahl gemeldeter Sicherheitsvorfälle durch Mitarbeiter

### 12.2.2 2.2 Compliance-KPIs

- Anzahl Audit-Findings (nach Schweregrad)
- Durchschnittliche Zeit zur Behebung von Findings
- Compliance-Rate mit Policies
- Anzahl Compliance-Verstöße

### 12.2.3 2.3 Operational-KPIs

- Uptime kritischer Systeme
- Backup-Erfolgsrate
- Restore-Test-Erfolgsrate
- Anzahl Change-Requests mit Sicherheitsreview

## 12.3 3. Messmethoden und Datenquellen

### 12.3.1 3.1 Datenquellen

KPI	Datenquelle	Verantwortlich	Automatisierung
Anzahl Incidents	Incident Management System	Security Team	Ja
Risikoscores	Risikoregister	ISMS Manager	Teilweise
Schwachstellen	Vulnerability Scanner	IT-Betrieb	Ja
Uptime	Monitoring-System	IT-Betrieb	Ja
Schulungsteilnahme	LMS	HR / CISO	Ja
Patch-Compliance	Patch Management System	IT-Betrieb	Ja

### 12.3.2 3.2 Reporting-Dashboards

**Monatliches Dashboard:** - Incident-Statistiken - Vulnerability-Status - Patch-Compliance - Uptime-Statistiken

**Quartalsweises Dashboard:** - Risiko-Übersicht - Audit-Findings-Status - Schulungs-Statistiken - Trend-Analysen

**Jährliches Dashboard:** - Zielerreichung - Jahresvergleich - Strategische Empfehlungen

## 12.4 4. Maßnahmen zur Zielerreichung

### 12.4.1 4.1 Verknüpfung zum Risikobehandlungsplan

Jedes Ziel ist mit Maßnahmen im Risikobehandlungsplan verknüpft: - Siehe 0090\_ISMS\_Risikobehandlungsplan\_P

**Beispiel:** - **Ziel Z-002:** Risiken minimieren - **Maßnahmen:** M-001 (Redundanter Switch), M-002 (Immutable Backups), M-003 (MFA-Rollout)

### 12.4.2 4.2 Kontinuierliche Verbesserung

**Verbesserungszyklus:** 1. Ziele definieren 2. Maßnahmen planen 3. Maßnahmen umsetzen 4. KPIs messen 5. Ergebnisse analysieren 6. Verbesserungen identifizieren 7. Ziele anpassen

## 12.5 5. Review und Anpassung

### 12.5.1 5.1 Regelmäßiger Review

**Quartalsweise:** - Review der KPI-Werte - Analyse von Abweichungen - Anpassung von Maßnahmen

**Jährlich:** - Vollständiger Review aller Ziele - Anpassung der Zielwerte - Definition neuer Ziele - Im Rahmen des Management Reviews

### 12.5.2 5.2 Trigger für außerplanmäßigen Review

- Wesentliche Änderungen im ISMS-Scope
- Neue Compliance-Anforderungen
- Major Security Incidents
- Audit-Findings

## 12.6 6. Referenzen

### 12.6.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register
- 0090\_ISMS\_Risikobehandlungsplan\_RTP\_Template.md - Risk Treatment Plan
- 0140\_ISMS\_Management\_Review\_Template.md - Management Review

### 12.6.2 Externe Standards

- ISO/IEC 27001:2022 - Clause 6.2: Information security objectives
- ISO/IEC 27001:2022 - Clause 9.1: Monitoring, measurement, analysis and evaluation

---

#### Genehmigt durch:

Thomas Weber, CISO

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 13

# Schulung, Awareness und Kompetenz

**Dokument-ID:** 0120

**Dokumenttyp:** ISMS-Grundlagendokument

**Standard-Referenz:** ISO/IEC 27001:2022 Clauses 7.2, 7.3

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

## 13.1 1. Zweck und Ziele

### 13.1.1 1.1 Zweck

Das Schulungs- und Awareness-Programm der **AdminSend GmbH** stellt sicher, dass: - Alle Mitarbeiter ihre Sicherheitsverantwortlichkeiten kennen - Mitarbeiter die notwendigen Kompetenzen für ihre Rollen haben - Sicherheitsbewusstsein kontinuierlich gefördert wird - Compliance mit ISO 27001:2022 und anderen Anforderungen sichergestellt wird

### 13.1.2 1.2 Ziele

- **100% Schulungsteilnahme:** Alle Mitarbeiter absolvieren jährlich Security Awareness Training
- **Phishing-Resilienz:** Klickrate bei Phishing-Simulationen < 5%
- **Incident Reporting:** Erhöhung der gemeldeten Sicherheitsvorfälle durch Mitarbeiter
- **Kompetenzaufbau:** Spezialisierte Schulungen für IT-Security-Rollen

## 13.2 2. Zielgruppen

### 13.2.1 2.1 Zielgruppen-Übersicht

Zielgruppe	Anzahl	Schulungsbedarf	Frequenz	Verantwortlich
Alle Mitarbeiter	<code>{{ meta.organization.employee_count }}</code>	Security Awareness Basics	Jährlich	Thomas Weber
Admins/Privileged Users	[TODO]	Advanced Security, Privileged Access	Halbjährlich	Thomas Weber
Entwickler/DevOps	[TODO]	Secure Coding, DevSecOps	Halbjährlich	Thomas Weber
Management	[TODO]	Security Governance, Risk Management	Jährlich	Thomas Weber
HR	[TODO]	HR Security, Onboarding/Offboarding	Jährlich	Thomas Weber
Dienstleister/Ext.	[TODO]	Security Basics, Compliance	Bei Onboarding	Thomas Weber

### 13.2.2 2.2 Rollenspezifische Anforderungen

**IT-Security-Team:** - ISO 27001 Lead Auditor Training - Incident Response Training - Threat Intelligence Training - Security Tool Training (SIEM, EDR, etc.)

**IT-Betrieb:** - Secure Configuration Management - Patch Management - Backup and Recovery - Access Management

**Entwickler:** - OWASP Top 10 - Secure Coding Practices - Secret Management - Security Testing (SAST/DAST)

## 13.3 3. Schulungsplan

### 13.3.1 3.1 Pflichtschulungen

Training-ID	Training	Zielgruppe	Frequenz	Dauer	Inhalt	Nachweis	Owner	Status
T-001	Security Awareness Basics	Alle Mitarbeiter	Jährlich	60 Min	Phishing, Passwörter, Clean Desk, Incident Reporting	LMS-Zertifikat	Thomas Weber	Aktiv
T-002	DSGVO Basics	Alle Mitarbeiter	Jährlich	30 Min	Datenschutz Grundlagen Betreuer-rechte	LMS-Zertifikat	<code>{{ meta.privacy.dpo }}</code>	Aktiv

Training-ID	Training	Zielgruppe	Frequenz	Dauer	Inhalt	Nachweis	Owner	Status
T-003	Phishing Awareness	Alle Mitarbeiter	Quartalsweise	15 Min	Phishing- Erkennung Mel- dung	Simulation- Ergebnis	Thomas Weber	Aktiv
T-004	Privileged Access Management	Admins	Halbjährlich	90 Min	PAM, Least Privilege, Audit Logging	LMS-Zertifikat	Thomas Weber	Aktiv
T-005	Secure Coding	Entwickler	Halbjährlich	120 Min	OWASP Top 10, Input Validation, Secrets	LMS-Zertifikat	Thomas Weber	Aktiv
T-006	Incident Response	Security Team	Jährlich	180 Min	IR-Prozess, Forensik, Kommunikation	Workshop- Teilnahme	Thomas Weber	Aktiv

[TODO: Weitere Schulungen hinzufügen]

### 13.3.2 3.2 Optionale Schulungen

Training	Zielgruppe	Frequenz	Anbieter	Kosten
ISO 27001 Lead Auditor	Security Team	Einmalig	Extern	[TODO]
CISSP/CISM Zertifizierung	Security Team	Einmalig	Extern	[TODO]
Cloud Security (AWS/Azure)	IT-Betrieb	Bei Bedarf	Extern	[TODO]
Penetration Testing	Security Team	Bei Bedarf	Extern	[TODO]

### 13.3.3 3.3 Onboarding-Schulungen

**Neue Mitarbeiter:** - Tag 1: Security Awareness Basics (T-001) - Tag 1: DSGVO Basics (T-002)  
- Woche 1: Rollenspezifische Schulungen

**Externe Dienstleister:** - Vor Zugriff: Security Basics - NDA-Unterzeichnung - Zugriffsrichtlinien

## 13.4 4. Awareness-Kampagnen

### 13.4.1 4.1 Regelmäßige Kampagnen

**Monatlich:** - Security Newsletter - Security Tip of the Month - Aktuelle Bedrohungen und Warnungen

**Quartalsweise:** - Phishing-Simulationen - Security Quiz mit Preisen - Lunch & Learn Sessions

**Jährlich:** - Security Awareness Month (Oktober) - Security Champions Program - Poster-Kampagnen

### 13.4.2 4.2 Themen-Schwerpunkte

Quartal	Thema	Aktivitäten
Q1	Passwort-Sicherheit	MFA-Rollout, Passwort-Manager-Training
Q2	Phishing & Social Engineering	Phishing-Simulation, Awareness-Videos
Q3	Mobile Security	BYOD-Policy, Mobile Device Management
Q4	Incident Response	Incident Reporting, Lessons Learned

### 13.4.3 4.3 Kommunikationskanäle

- **E-Mail:** Security Newsletter, Warnungen
- **Intranet:** Security-Portal, Policies, FAQs
- **Poster:** Büros, Pausenräume
- **Teams/Slack:** Security-Channel
- **Workshops:** Lunch & Learn, Hands-on-Training

## 13.5 5. Phishing-Simulationen

### 13.5.1 5.1 Simulationsprogramm

**Frequenz:** Quartalsweise

**Prozess:** 1. Simulation planen (Thema, Zielgruppe) 2. Phishing-E-Mail versenden 3. Klickrate messen 4. Sofortiges Feedback für Klicker 5. Nachschulung für Risikogruppen 6. Ergebnisse analysieren und berichten

**Zielwerte:** - Klickrate < 5% - Melderate > 50%

**Tools:** - [TODO: KnowBe4, Cofense, etc.]

### 13.5.2 5.2 Eskalation bei hoher Klickrate

**Klickrate > 10%:** - Zusätzliche Awareness-Kampagne - Verpflichtende Nachschulung - Analyse der Ursachen

**Klickrate > 20%:** - Eskalation an Management - Intensivierte Schulungsmaßnahmen - Review des Awareness-Programms

## 13.6 6. Wirksamkeitsprüfung

### 13.6.1 6.1 Messmethoden

**Quantitative Metriken:** - Schulungsteilnahme-Quote - Phishing-Klickrate - Quiz-Ergebnisse - Anzahl gemeldeter Incidents durch Mitarbeiter - Anzahl Sicherheitsverstöße

**Qualitative Metriken:** - Feedback-Umfragen - Interviews mit Stakeholdern - Beobachtungen (Clean Desk, Screen Lock)

### 13.6.2 6.2 Erfolgskriterien

Metrik	Zielwert	Aktuell	Status
Schulungsteilnahme	100%	[TODO]%	[TODO]
Phishing-Klickrate	< 5%	[TODO]%	[TODO]
Incident-Meldungen	> 20 pro Quartal	[TODO]	[TODO]
Quiz-Erfolgsrate	> 80%	[TODO]%	[TODO]

### 13.6.3 6.3 Kontinuierliche Verbesserung

**Jährlicher Review:** - Analyse der Schulungsergebnisse - Feedback-Auswertung - Anpassung der Schulungsinhalte - Identifikation neuer Themen

**Lessons Learned:** - Aus Security Incidents - Aus Audit-Findings - Aus Phishing-Simulationen

## 13.7 7. Schulungsnachweise

### 13.7.1 7.1 Dokumentation

**Learning Management System (LMS):** - Schulungsteilnahme - Zertifikate - Quiz-Ergebnisse - Ablaufdaten

**Manuelle Nachweise:** - Workshop-Teilnahmelisten - Externe Zertifikate - Konferenz-Teilnahmen

### 13.7.2 7.2 Aufbewahrung

**Aufbewahrungsfrist:** 10 Jahre

**Zugriff:** - HR: Alle Nachweise - CISO: Alle Nachweise - Manager: Nachweise ihres Teams - Mitarbeiter: Eigene Nachweise

### 13.7.3 7.3 Audit-Nachweise

Für Audits werden folgende Nachweise bereitgestellt: - Schulungsplan - Teilnahmelisten - Zertifikate - Phishing-Simulationsergebnisse - Awareness-Kampagnen-Dokumentation

## 13.8 8. Rollen und Verantwortlichkeiten

### 13.8.1 8.1 RACI-Matrix: Schulung und Awareness

Aktivität	CISO	HR	Manager	Mitarbeiter	Externe Trainer
Schulungsplan erstellen	R/A	C	C	I	I
Schulungen durchführen	R	C	I	I	R
Teilnahme sicherstellen	A	C	R	R	I
Nachweise dokumentieren	A	R	C	I	I
Wirksamkeit prüfen	R/A	C	C	I	I
Awareness-Kampagnen	R/A	C	C	I	C
Phishing-Simulationen	R/A	I	I	I	C

**Legende:** R = Responsible, A = Accountable, C = Consulted, I = Informed

### 13.8.2 8.2 Security Champions

**Programm:** - Freiwillige Mitarbeiter aus allen Abteilungen - Multiplikatoren für Security Awareness - Regelmäßige Treffen und Schulungen - Anerkennung und Incentives

**Aufgaben:** - Awareness in ihren Teams fördern - Fragen zu Security beantworten - Feedback an Security Team - Teilnahme an Security-Projekten

## 13.9 9. Budget und Ressourcen

### 13.9.1 9.1 Budgetplanung

Kategorie	Jährliches Budget	Bemerkungen
LMS-Lizenz	[TODO] €	E-Learning-Plattform
Externe Schulungen	[TODO] €	Zertifizierungen, Konferenzen
Phishing-Simulation-Tool	[TODO] €	KnowBe4, Cofense, etc.
Awareness-Material	[TODO] €	Poster, Flyer, Giveaways
Externe Trainer	[TODO] €	Workshops, Spezialschulungen
<b>Gesamt</b>	<b>[TODO] €</b>	

### 13.9.2 9.2 Zeitressourcen

**CISO/Security Team:** - Schulungsplanung: 20 PT/Jahr - Schulungsdurchführung: 40 PT/Jahr  
- Awareness-Kampagnen: 30 PT/Jahr - Phishing-Simulationen: 20 PT/Jahr

**Mitarbeiter:** - Pflichtschulungen: 2 Stunden/Jahr - Optionale Schulungen: Nach Bedarf

## 13.10 10. Referenzen

### 13.10.1 10.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0040\_ISMS\_Governance\_Rollen\_und\_Verantwortlichkeiten.md - Governance
- 0110\_ISMS\_Sicherheitsziele\_und\_Metriken.md - Security Objectives
- 0200\_Policy\_Akzeptable\_Nutzung\_IT.md - Acceptable Use Policy
- 0520\_Policy\_HR\_Security.md - HR Security

### **13.10.2 10.2 Externe Standards**

- ISO/IEC 27001:2022 - Clause 7.2: Competence
  - ISO/IEC 27001:2022 - Clause 7.3: Awareness
  - ISO/IEC 27002:2022 - Control 6.3: Information security awareness, education and training
- 

**Genehmigt durch:**

Thomas Weber, CISO

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 14

## Internes Auditprogramm (Template)

**Dokument-ID:** 0130

**Dokumenttyp:** ISMS-Programm/Template

**Standard-Referenz:** ISO/IEC 27001:2022 Clause 9.2

**Owner:** {{ meta.audit.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Vertraulich

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 14.1 1. Zweck und Geltungsbereich

#### 14.1.1 1.1 Zweck

Das interne Auditprogramm der **AdminSend GmbH** stellt sicher, dass: - Das ISMS den Anforderungen von ISO 27001:2022 entspricht - Das ISMS wirksam implementiert und aufrechterhalten wird - Verbesserungspotenziale identifiziert werden - Compliance mit Policies und Richtlinien sichergestellt wird

#### 14.1.2 1.2 Geltungsbereich

Das Auditprogramm umfasst: - Alle Bereiche im ISMS-Scope (siehe 0020\_ISMS\_Geltungsbereich\_Scope.md)  
- Alle Annex A Controls im SoA (siehe 0100\_ISMS\_Statement\_of\_Applicability\_SoA\_Template.md)  
- Alle ISMS-Prozesse und -Dokumente - Alle Standorte: {{ netbox.site.name }} und weitere

### 14.2 2. Audit-Ansatz

#### 14.2.1 2.1 Audit-Prinzipien

**Unabhängigkeit:** - Auditoren prüfen nicht ihre eigenen Bereiche - Externe Auditoren für kritische Bereiche (optional) - Berichtslinie: Audit-Team berichtet an {{ meta.audit.manager }}

**Risikobasiert:** - Audit-Frequenz basiert auf Risikobewertung - Kritische Bereiche werden häufiger geprüft - Fokus auf hohe Risiken und kritische Controls

**Scope-bezogen:** - Alle Bereiche im ISMS-Scope werden geprüft - Vollständige Abdeckung innerhalb des Audit-Zyklus (3 Jahre)

**Objektiv und evidenzbasiert:** - Audit-Findings basieren auf objektiven Nachweisen - Stichprobenbasierte Prüfung - Dokumentation aller Findings

## 14.2.2 2.2 Audit-Typen

**Vollständiges ISMS-Audit:** - Frequenz: Jährlich - Scope: Gesamtes ISMS - Dauer: 5-10 Tage

**Themen-Audits:** - Frequenz: Quartalsweise - Scope: Spezifische Themen (z.B. Access Management, Patch Management) - Dauer: 1-2 Tage

**Follow-up-Audits:** - Frequenz: Nach Bedarf - Scope: Überprüfung der Umsetzung von Korrekturmaßnahmen - Dauer: 0,5-1 Tag

## 14.3 3. Jahresplan

### 14.3.1 3.1 Audit-Jahresplan 2026

Zeitraum	Audit-Thema/Scope	Audit-Typ	Kriterien	Auditor	Auditee	Geplante Dauer	Status
<b>Q1 2026</b>	Access Management & IAM	Themen-Audit	A.5.15, A.5.16, A.5.17, A.5.18, A.8.2, A.8.3	[TODO]	Anna Schmidt	2 Tage	Geplant
<b>Q2 2026</b>	Vulnerability & Patch Management	Themen-Audit	A.8.8, A.5.23	[TODO]	IT-Betrieb	1 Tag	Geplant
<b>Q3 2026</b>	Vollständiges ISMS-Audit	Vollaudit	Alle Clauses, SoA	[TODO]	Thomas Weber	10 Tage	Geplant
<b>Q4 2026</b>	Incident Management & Logging	Themen-Audit	A.5.24, A.5.25, A.5.26, A.5.28, A.8.15, A.8.16	[TODO]	Security Team	2 Tage	Geplant

[TODO: Audit-Plan für 2026 vervollständigen]

### 14.3.2 3.2 Audit-Frequenz nach Risiko

Bereich	Risikostufe	Audit-Frequenz
Privileged Access Management	Hoch	Halbjährlich
Vulnerability Management	Hoch	Halbjährlich
Incident Management	Hoch	Halbjährlich
Backup & Recovery	Mittel	Jährlich
Physical Security	Mittel	Jährlich
HR Security	Niedrig	Alle 2 Jahre

## 14.4 4. Audit-Prozess

### 14.4.1 4.1 Audit-Phasen

#### 1. Planung

- Audit-Scope definieren
- Audit-Team benennen
- Audit-Plan erstellen
- Auditee informieren

#### 2. Vorbereitung

- Dokumente anfordern
- Audit-Checkliste erstellen
- Stichproben definieren
- Interviews planen

#### 3. Durchführung

- Opening Meeting
- Dokumentenprüfung
- Interviews
- Stichproben
- Beobachtungen
- Closing Meeting

#### 4. Berichterstattung

- Findings dokumentieren
- Audit-Bericht erstellen
- Bericht an Auditee
- Bericht an Management

#### 5. Follow-up

- Korrekturmaßnahmen planen
- Umsetzung überwachen
- Follow-up-Audit
- Findings schließen

### 14.4.2 4.2 Audit-Checkliste (Beispiel)

**Audit-Thema:** Access Management

Prüfpunkt	Kriterium	Nachweis	Ergebnis	Bemerkungen
Sind Zugriffsrechte dokumentiert?	Policy 0220	IAM-Dokumentation	/	
Werden Zugriffsrechte regelmäßig rezertifiziert?	Richtlinie 0230	Rezertifizierungsprotokolle		
Ist das Least-Privilege-Prinzip umgesetzt?	A.8.2	IAM-Konfiguration	/	
Werden Joiner/Mover/Leaver-Prozesse befolgt?	Richtlinie 0230	HR-Tickets, IAM-Logs	/	
Ist MFA für alle Benutzer aktiviert?	A.5.17	MFA-Konfiguration	/	

[TODO: Vollständige Checklisten für alle Audit-Themen erstellen]

#### 14.4.3 4.3 Audit-Kriterien

**Dokumentenprüfung:** - Sind Dokumente aktuell und freigegeben? - Sind Dokumente vollständig und konsistent? - Sind Verantwortlichkeiten definiert?

**Evidence-Prüfung:** - Ist Evidence vorhanden und aktuell? - Ist Evidence nachvollziehbar? - Ist Evidence ausreichend für Nachweis?

**Control-Wirksamkeit:** - Ist das Control implementiert? - Ist das Control wirksam (Stichproben)? - Gibt es Abweichungen oder Schwachstellen?

**Compliance:** - Werden Policies und Richtlinien befolgt? - Werden gesetzliche Anforderungen erfüllt? - Werden vertragliche Verpflichtungen erfüllt?

### 14.5 5. Audit-Findings

#### 14.5.1 5.1 Finding-Kategorien

**Major Non-Conformity (Schwerwiegend):** - Wesentlicher Verstoß gegen ISO 27001:2022 - Kritisches Control nicht implementiert - Systemischer Fehler - **Beispiel:** Keine Risikoanalyse durchgeführt

**Minor Non-Conformity (Geringfügig):** - Kleinerer Verstoß gegen ISO 27001:2022 - Control teilweise implementiert - Isolierter Fehler - **Beispiel:** Dokumentation unvollständig

**Observation (Beobachtung):** - Verbesserungspotenzial - Best Practice nicht umgesetzt - Kein Verstoß gegen Anforderungen - **Beispiel:** Prozess könnte effizienter sein

**Opportunity for Improvement (Verbesserungsmöglichkeit):** - Empfehlung für Verbesserung - Keine Abweichung - **Beispiel:** Automatisierung möglich

## **14.5.2 5.2 Finding-Dokumentation**

**Für jedes Finding:** - Finding-ID (z.B. F-2026-Q1-001) - Kategorie (Major/Minor/Observation) - Beschreibung - Betroffener Bereich/Control - Nachweis/Evidence - Auswirkung - Empfohlene Korrekturmaßnahme - Verantwortlicher - Frist

## **14.5.3 5.3 Korrekturmaßnahmen**

**Prozess:** 1. Auditee plant Korrekturmaßnahme 2. CISO genehmigt Maßnahme und Frist 3. Auditee setzt Maßnahme um 4. Auditor prüft Umsetzung (Follow-up) 5. Finding wird geschlossen

**Fristen:** - Major Non-Conformity: 30 Tage - Minor Non-Conformity: 90 Tage - Observation: 180 Tage

# **14.6 6. Audit-Bericht**

## **14.6.1 6.1 Berichtsstruktur**

**Executive Summary:** - Audit-Scope und -Ziel - Audit-Datum und -Team - Zusammenfassung der Ergebnisse - Gesamtbewertung

**Audit-Details:** - Audit-Methodik - Geprüfte Bereiche und Controls - Stichproben - Interviews

**Findings:** - Liste aller Findings (nach Kategorie) - Detailbeschreibung jedes Findings - Empfohlene Korrekturmaßnahmen

**Positive Beobachtungen:** - Best Practices - Gut umgesetzte Controls - Verbesserungen seit letztem Audit

**Schlussfolgerung:** - Gesamtbewertung des ISMS - Empfehlungen - Nächste Schritte

## **14.6.2 6.2 Berichtsverteilung**

**Empfänger:** - Auditee - CISO - Geschäftsführung - Informationssicherheitsgremium

**Vertraulichkeit:** - Audit-Berichte sind vertraulich - Zugriff nur für berechtigte Personen

# **14.7 7. Auditor-Qualifikation**

## **14.7.1 7.1 Anforderungen an Auditoren**

**Fachliche Qualifikation:** - Kenntnisse ISO 27001:2022 - Kenntnisse ISO 27002:2022 - Kenntnisse Audit-Methodik - Branchenkenntnisse

**Zertifizierungen (empfohlen):** - ISO 27001 Lead Auditor - CISA (Certified Information Systems Auditor) - CISM (Certified Information Security Manager)

**Soft Skills:** - Kommunikationsfähigkeit - Objektivität - Analytisches Denken - Dokumentationsfähigkeit

## **14.7.2 7.2 Auditor-Training**

**Initiales Training:** - ISO 27001:2022 Schulung - Audit-Methodik-Schulung - Shadowing erfahrener Auditoren

**Kontinuierliche Weiterbildung:** - Jährliche Auffrischung - Teilnahme an Auditor-Konferenzen - Austausch mit anderen Auditoren

## 14.8 8. Audit-Metriken

### 14.8.1 8.1 KPIs

Metrik	Zielwert	Aktuell	Status
Audit-Plan-Erfüllung	100%	[TODO]%	[TODO]
Durchschnittliche Zeit zur Behebung (Major)	< 30 Tage	[TODO] Tage	[TODO]
Durchschnittliche Zeit zur Behebung (Minor)	< 90 Tage	[TODO] Tage	[TODO]
Anzahl offener Findings	< 5	[TODO]	[TODO]
Wiederkehrende Findings	0	[TODO]	[TODO]

### 14.8.2 8.2 Trend-Analyse

**Jährlicher Review:** - Anzahl Findings pro Jahr (Trend) - Häufigste Finding-Kategorien - Bereiche mit den meisten Findings - Verbesserungen seit Vorjahr

## 14.9 9. Rollen und Verantwortlichkeiten

### 14.9.1 9.1 RACI-Matrix: Audit-Prozess

Aktivität	Audit Manager	Auditor	Auditee	CISO	Geschäftsführung
Audit-Programm erstellen	R/A	C	C	C	I
Audit planen	R	R	C	I	I
Audit durchführen	A	R	C	I	I
Findings dokumentieren	A	R	C	I	I
Audit-Bericht erstellen	R/A	R	C	I	I
Korrekturmaßnahmen planen		C	R/A	C	I
Follow-up durchführen	A	R	C	I	I

Aktivität	Audit Manager	Auditor	Auditee	CISO	Geschäftsführung
Audit- Programm reviewen	R/A	C	C	C	C

**Legende:** R = Responsible, A = Accountable, C = Consulted, I = Informed

## 14.10 10. Referenzen

### 14.10.1 10.1 Interne Dokumente

- 0020\_ISMS\_Geltungsbereich\_Scope.md - ISMS Scope
- 0100\_ISMS\_Statement\_of\_Applicability\_SoA\_Template.md - SoA
- 0140\_ISMS\_Management\_Review\_Template.md - Management Review
- 0150\_ISMS\_Nichtkonformitaeten\_und\_Korrekturmassnahmen.md - Non-conformities
- Alle Policies (0200-0680) und Richtlinien (0210-0690)

### 14.10.2 10.2 Externe Standards

- ISO/IEC 27001:2022 - Clause 9.2: Internal audit
- ISO 19011:2018 - Guidelines for auditing management systems
- ISO/IEC 27007:2020 - Guidelines for information security management systems auditing

---

#### Genehmigt durch:

{{ meta.audit.manager }}, Audit Manager

Thomas Weber, CISO

Datum: {{ meta.document.approval\_date }}

Nächster Review: {{ meta.document.next\_review }}

ewpage

# Chapter 15

## Management Review (Template)

**Dokument-ID:** 0140

**Dokumenttyp:** ISMS-Nachweis/Template

**Standard-Referenz:** ISO/IEC 27001:2022 Clause 9.3

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Vertraulich

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 15.1 1. Management Review-Übersicht

#### 15.1.1 1.1 Teilnehmer und Zeitraum

**Review-Datum:** [TODO: Datum]

**Review-Zeitraum:** [TODO: z.B. 01.01.2026 - 31.12.2026]

**Nächster Review:** [TODO: Datum]

**Teilnehmer:**

Name	Rolle	Anwesend
{{ meta.management.ceo }}	Geschäftsführung (Vorsitz)	/
Thomas Weber	CISO	/
Anna Schmidt	CIO	/
[TODO]	CFO	/
[TODO]	Vertreter Fachabteilungen	/
{{ meta.audit.manager }}	Internal Audit (beratend)	/

#### 15.1.2 1.2 Scope

Dieser Management Review umfasst: - Gesamtes ISMS im Scope (siehe 0020\_ISMS\_Geltungsbereich\_Scope.md)  
- Alle Standorte: {{ netbox.site.name }} und weitere - Review-Zeitraum: [TODO]

## 15.2 2. Inputs (Clause 9.3.2)

### 15.2.1 2.1 Status der Maßnahmen aus vorherigem Review

Maßnahmen aus letztem Review ([TODO: Datum]):

Maßnahme	Verantwortlich	Frist	Status	Bemerkungen
[TODO]	[TODO]	[TODO]	Abgeschlossen / In Arbeit / Offen	[TODO]

**Zusammenfassung:** - Abgeschlossen: [TODO] von [TODO] - In Arbeit: [TODO] - Offen/Überfällig: [TODO]

### 15.2.2 2.2 Änderungen bei externen und internen Themen

**Externe Änderungen:** - **Regulatorische Änderungen:** [TODO: z.B. NIS2-Umsetzung, DSGVO-Updates] - **Bedrohungslage:** [TODO: z.B. Neue Ransomware-Varianten, APT-Aktivitäten] - **Marktentwicklung:** [TODO: z.B. Neue Wettbewerber, Kundenanforderungen] - **Technologietrends:** [TODO: z.B. Cloud-Migration, KI-Einsatz]

**Interne Änderungen:** - **Organisatorisch:** [TODO: z.B. Merger, Akquisitionen, Umstrukturierungen] - **Personell:** [TODO: z.B. Neue CISO, Teamvergrößerung] - **Technologisch:** [TODO: z.B. Neue Systeme, Cloud-Migration] - **Prozesse:** [TODO: z.B. DevOps-Einführung, Agile Transformation]

**Auswirkungen auf ISMS:** - Scope-Änderungen erforderlich: Ja / Nein - Risikoanalyse-Update erforderlich: Ja / Nein - Policy-Updates erforderlich: Ja / Nein

### 15.2.3 2.3 Feedback zu Informationssicherheitsleistung

**KPI-Entwicklung:**

KPI	Zielwert	Aktuell	Vorjahr	Trend	Status
Anzahl Security Incidents	< 10/Quartal	[TODO]	[TODO]	↑ / → / ↓	/
Risiken mit Score 13	< 5	[TODO]	[TODO]	↑ / → / ↓	/
Uptime kritischer Systeme	99,5%	[TODO]%	[TODO]%	↑ / → / ↓	/

KPI	Zielwert	Aktuell	Vorjahr	Trend	Status
Patch-Compliance (kritisch)	< 7 Tage	[TODO] Tage	[TODO] Tage	↑ / → / ↓	/
Schulungsteilnahme	100%	[TODO]%	[TODO]%	↑ / → / ↓	/
Phishing-Klickrate	< 5%	[TODO]%	[TODO]%	↑ / → / ↓	/

**Zusammenfassung:** - Ziele erreicht: [TODO] von [TODO] - Verbesserungen: [TODO] - Verschlechterungen: [TODO]

**Stakeholder-Feedback:** - Kunden: [TODO] - Mitarbeiter: [TODO] - Aufsichtsbehörden: [TODO]  
- Lieferanten: [TODO]

#### 15.2.4 2.4 Ergebnisse interner und externer Audits

##### Interne Audits:

Audit-Datum	Scope	Findings (Major/Minor/Obs)	Status	Bemerkungen
[TODO]	Access Management	0 / 2 / 3	Abgeschlossen	All findings resolved
[TODO]	Vulnerability Management	1 / 2	In Arbeit	Major finding under review
[TODO]	Vollständigkeit ISMS	8 / 5 / 8	Abgeschlossen	Improvements implemented

##### Externe Audits:

Audit-Datum	Auditor	Scope	Ergebnis	Zertifikat	Bemerkungen
[TODO]	[TODO: Zertifizierungsstelle]	ISO 27001:2022	Bestanden	Gültig bis [TODO]	Rezertifizierung erfolgreich

**Zusammenfassung:** - Offene Major Findings: [TODO] - Offene Minor Findings: [TODO] - Durchschnittliche Behebungzeit: [TODO] Tage

#### 15.2.5 2.5 Feedback von interessierten Parteien

**Kunden:** - Sicherheitsanforderungen: [TODO] - Zufriedenheit: [TODO] - Incidents mit Kundenauswirkung: [TODO]

**Aufsichtsbehörden:** - Meldepflichtige Vorfälle: [TODO] - Compliance-Status: [TODO]

**Lieferanten:** - Third-Party-Risiken: [TODO] - Sicherheitsvorfälle bei Lieferanten: [TODO]

## 15.2.6 2.6 Ergebnisse der Risikobewertung

### Risiko-Übersicht:

Risikostufe	Anzahl Risiken	Vorjahr	Trend
Sehr hoch	[TODO]	[TODO]	↑ / → / ↓
Hoch	[TODO]	[TODO]	↑ / → / ↓
Mittel	[TODO]	[TODO]	↑ / → / ↓
Niedrig	[TODO]	[TODO]	↑ / → / ↓

### Top 5 Risiken:

Risiko-ID	Beschreibung	Score	Behandlung	Status
R-001	[TODO]	[TODO]	[TODO]	[TODO]
R-002	[TODO]	[TODO]	[TODO]	[TODO]
R-003	[TODO]	[TODO]	[TODO]	[TODO]
R-004	[TODO]	[TODO]	[TODO]	[TODO]
R-005	[TODO]	[TODO]	[TODO]	[TODO]

**Neue Risiken:** - [TODO: Liste neuer Risiken seit letztem Review]

**Geschlossene Risiken:** - [TODO: Liste geschlossener Risiken]

## 15.2.7 2.7 Möglichkeiten zur kontinuierlichen Verbesserung

### Identifizierte Verbesserungsmöglichkeiten:

ID	Bereich	Verbesserung	Nutzen	Aufwand	Priorität
V-001	[TODO]	[TODO]	[TODO]	[TODO]	Hoch / Mittel / Niedrig
V-002	[TODO]	[TODO]	[TODO]	[TODO]	Hoch / Mittel / Niedrig

**Lessons Learned:** - Aus Security Incidents: [TODO] - Aus Audits: [TODO] - Aus Projekten: [TODO]

## 15.2.8 2.8 Relevante Änderungen

**ISMS-Scope:** - Änderungen: [TODO: Neue Standorte, Systeme, Prozesse] - Auswirkungen: [TODO]

**Technologie:** - Neue Systeme: [TODO] - Cloud-Migration: [TODO] - Technologie-Refresh: [TODO]

**Lieferanten:** - Neue kritische Lieferanten: [TODO] - Beendete Lieferantenbeziehungen: [TODO]

**Personal:** - Neue Schlüsselpersonen: [TODO] - Abgänge: [TODO]

## 15.2.9 2.9 Incidents und Lessons Learned

### Security Incidents:

Incident-ID	Datum	Schweregrad	Beschreibung	Auswirkung	Lessons Learned	Status
INC-001	[TODO]	Hoch	[TODO]	[TODO]	[TODO]	Geschlossen
INC-002	[TODO]	Mittel	[TODO]	[TODO]	[TODO]	Geschlossen

**Zusammenfassung:** - Anzahl Incidents: [TODO] - Major Incidents: [TODO] - MTTD (Mean Time to Detect): [TODO] - MTTR (Mean Time to Respond): [TODO]

**Umgesetzte Verbesserungen:** - [TODO: Maßnahmen aus Lessons Learned]

## 15.2.10 2.10 Ressourcen

**Budget:** - Geplantes Budget: [TODO] € - Tatsächliche Ausgaben: [TODO] € - Abweichung: [TODO] € ([TODO]%)

**Personal:** - Geplante FTE: [TODO] - Tatsächliche FTE: [TODO] - Engpässe: [TODO]

**Externe Unterstützung:** - Berater: [TODO] - Managed Services: [TODO] - Schulungen: [TODO]

## 15.3 3. Outputs / Entscheidungen (Clause 9.3.3)

### 15.3.1 3.1 Anpassungen an ISMS-Leitlinie und Zielen

**ISMS-Leitlinie:** - Änderungen erforderlich: Ja / Nein - Beschreibung: [TODO] - Verantwortlich: Thomas Weber - Frist: [TODO]

**Sicherheitsziele:** - Neue Ziele: [TODO] - Anpassung bestehender Ziele: [TODO] - Verantwortlich: Thomas Weber - Frist: [TODO]

### 15.3.2 3.2 Ressourcen und Investitionen

#### Genehmigte Investitionen:

Investition	Beschreibung	Budget	Verantwortlich	Frist	Priorität
[TODO]	[TODO]	[TODO] €	[TODO]	[TODO]	Hoch / Mittel / Niedrig

**Personalressourcen:** - Zusätzliche FTE: [TODO] - Externe Unterstützung: [TODO] - Schulungsbudget: [TODO] €

### 15.3.3 3.3 Verbesserungsmaßnahmen

#### Beschlossene Maßnahmen:

Maßnahme-ID	Maßnahme	Ziel	Verantwortlich	Frist	Budget	Status
M-001	[TODO]	[TODO]	[TODO]	[TODO]	[TODO] €	Genehmigt
M-002	[TODO]	[TODO]	[TODO]	[TODO]	[TODO] €	Genehmigt

### 15.3.4 3.4 Akzeptierte Risiken

Risikoakzeptanz durch Geschäftsführung:

Risiko-ID	Beschreibung	Score	Begründung	Gültig bis	Kompensationsmaßnahmen
R-010	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

### 15.3.5 3.5 Scope-Änderungen

**Beschlossene Scope-Änderungen:** - [TODO: Neue Standorte, Systeme, Prozesse] - Auswirkungen auf Risikoanalyse: [TODO] - Auswirkungen auf SoA: [TODO] - Verantwortlich: Thomas Weber - Frist: [TODO]

### 15.3.6 3.6 Strategische Entscheidungen

**Strategische Ausrichtung:** - [TODO: z.B. Cloud-First-Strategie, Zero-Trust-Architektur]

**Compliance-Strategie:** - [TODO: z.B. NIS2-Vorbereitung, zusätzliche Zertifizierungen]

**Sicherheitskultur:** - [TODO: z.B. Security Champions Program, Awareness-Kampagnen]

## 15.4 4. Zusammenfassung und Bewertung

### 15.4.1 4.1 Gesamtbewertung des ISMS

**Eignung (Suitability):** - Das ISMS ist geeignet für die Organisation: Ja / Nein / Teilweise - Begründung: [TODO]

**Angemessenheit (Adequacy):** - Das ISMS ist angemessen für die Risiken: Ja / Nein / Teilweise - Begründung: [TODO]

**Wirksamkeit (Effectiveness):** - Das ISMS ist wirksam: Ja / Nein / Teilweise - Begründung: [TODO]

**Gesamtbewertung:** - [TODO: Zusammenfassende Bewertung durch Geschäftsführung]

### 15.4.2 4.2 Nächste Schritte

1. [TODO: Maßnahme 1]
2. [TODO: Maßnahme 2]
3. [TODO: Maßnahme 3]

**Nächster Management Review:** [TODO: Datum]

## 15.5 5. Anhänge

### 15.5.1 5.1 Unterstützende Dokumente

- Risikoregister (0080\_ISMS\_Risikoregister\_Template.md)
- Risikobehandlungsplan (0090\_ISMS\_Risikobehandlungsplan\_RTP\_Template.md)
- Audit-Berichte (0130\_ISMS\_Internes\_Auditprogramm.md)
- KPI-Dashboard (0110\_ISMS\_Sicherheitsziele\_und\_Metriken.md)
- Incident Reports (0400\_Policy\_Incident\_Management.md)

### 15.5.2 5.2 Präsentationen

- [TODO: Link zu Management Review Präsentation]

## 15.6 6. Referenzen

### 15.6.1 6.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0020\_ISMS\_Geltungsbereich\_Scope.md - ISMS Scope
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register
- 0090\_ISMS\_Risikobehandlungsplan\_RTP\_Template.md - Risk Treatment Plan
- 0110\_ISMS\_Sicherheitsziele\_und\_Metriken.md - Security Objectives
- 0130\_ISMS\_Internes\_Auditprogramm.md - Internal Audit Program

### 15.6.2 6.2 Externe Standards

- ISO/IEC 27001:2022 - Clause 9.3: Management review
- ISO/IEC 27002:2022 - Information security controls

---

## 15.7 Änderungshistorie

Version	Datum	Autor	Beschreibung	Genehmigt durch
1.0	{} meta.document.Wdate {}}	Thomas	Initiale Version	{} {{ meta.management.ceo }} }}

---

### Protokolliert durch:

Thomas Weber, CISO

Datum: [TODO]

### Genehmigt durch:

{}{{ meta.management.ceo }}, Geschäftsführung

Datum: [TODO]

Nächster Review: [TODO: Datum] (Jährlich)

ewpage

# Chapter 16

## Nichtkonformitäten und Korrekturmaßnahmen

**Dokument-ID:** 0150

**Dokumenttyp:** ISMS-Prozess/Template

**Standard-Referenz:** ISO/IEC 27001:2022 Clause 10.1

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 16.1 1. Zweck und Ziel

#### 16.1.1 1.1 Zweck

Dieses Dokument definiert den Prozess zur systematischen Behandlung von Nichtkonformitäten (Non-Conformities) im ISMS der **AdminSend GmbH**. Es stellt sicher, dass: - Abweichungen von Anforderungen erkannt und dokumentiert werden - Ursachen analysiert und behoben werden - Korrekturmaßnahmen wirksam umgesetzt werden - Wiederholungen verhindert werden

#### 16.1.2 1.2 Arten von Nichtkonformitäten

**Audit-Findings:** - Major Non-Conformities (schwerwiegend) - Minor Non-Conformities (geringfügig) - Observations (Beobachtungen)

**Security Incidents:** - Sicherheitsvorfälle mit Ursache in Prozess-/Control-Schwächen

**Policy-Verstöße:** - Verstöße gegen ISMS-Policies und -Richtlinien

**Compliance-Verstöße:** - Verstöße gegen gesetzliche oder vertragliche Anforderungen

## 16.2 2. Prozess

### 16.2.1 2.1 Prozessübersicht

#### 1. Erfassen

- Nichtkonformität identifizieren
- Ticket/Finding erstellen
- Kategorisieren und priorisieren

#### 2. Ursachenanalyse

- Root Cause Analysis durchführen
- Beitragende Faktoren identifizieren
- Systemische Ursachen erkennen

#### 3. Korrekturmaßnahme definieren

- Sofortmaßnahme (Containment)
- Korrekturmaßnahme (Corrective Action)
- Präventivmaßnahme (Preventive Action)

#### 4. Umsetzung

- Maßnahme implementieren
- Fortschritt tracken
- Dokumentieren

#### 5. Wirksamkeitsprüfung

- Wirksamkeit verifizieren
- Follow-up durchführen
- Lessons Learned dokumentieren

#### 6. Abschluss

- Finding schließen
- Dokumentation archivieren
- Kommunikation

### 16.2.2 2.2 Schritt 1: Erfassen

**Identifikation:** - Durch Audits (intern/extern) - Durch Security Incidents - Durch Monitoring und KPIs - Durch Mitarbeiter-Meldungen - Durch Management Reviews

**Dokumentation:** - Finding-ID vergeben (z.B. F-2026-001) - Beschreibung der Nichtkonformität - Betroffener Bereich/Control - Nachweis/Evidence - Kategorisierung (Major/Minor/Observation) - Priorität (Hoch/Mittel/Niedrig)

**Verantwortlich:** Auditor, ISMS Manager, oder Melder

### 16.2.3 2.3 Schritt 2: Ursachenanalyse

**Root Cause Analysis (RCA):** - **5-Why-Methode:** Warum ist das passiert? (5x fragen) -

**Fishbone-Diagramm:** Ursachen-Kategorien (Mensch, Prozess, Technologie, Umgebung) - **Fault Tree Analysis:** Logische Analyse von Fehlerursachen

**Zu identifizieren:** - Direkte Ursache (Immediate Cause) - Grundursache (Root Cause) - Beitragende Faktoren (Contributing Factors) - Systemische Ursachen (Systemic Causes)

**Dokumentation:** - RCA-Methode - Identifizierte Ursachen - Beitragende Faktoren

**Verantwortlich:** Finding-Owner, unterstützt durch ISMS Manager

#### 16.2.4 2.4 Schritt 3: Korrekturmaßnahme definieren

**Sofortmaßnahme (Immediate Action):** - Eindämmung des Problems - Schadensbegrenzung - Temporäre Lösung

**Korrekturmaßnahme (Corrective Action):** - Behebung der Grundursache - Dauerhafte Lösung - Prozess-/Control-Verbesserung

**Präventivmaßnahme (Preventive Action):** - Verhinderung von Wiederholungen - Verhindern ähnlicher Probleme - Systemische Verbesserungen

**Dokumentation:** - Beschreibung der Maßnahme - Verantwortlicher - Frist - Ressourcen/Budget - Erfolgskriterien

**Verantwortlich:** Finding-Owner, genehmigt durch CISO

#### 16.2.5 2.5 Schritt 4: Umsetzung

**Implementierung:** - Maßnahme gemäß Plan umsetzen - Fortschritt dokumentieren - Stakeholder informieren

**Tracking:** - Regelmäßige Status-Updates - Eskalation bei Verzögerungen - Anpassung bei Problemen

**Dokumentation:** - Umsetzungsschritte - Abweichungen vom Plan - Lessons Learned

**Verantwortlich:** Finding-Owner

#### 16.2.6 2.6 Schritt 5: Wirksamkeitsprüfung

**Verifikation:** - Ist die Maßnahme umgesetzt? - Ist die Nichtkonformität behoben? - Ist die Grundursache beseitigt?

**Validierung:** - Ist die Maßnahme wirksam? - Tritt das Problem noch auf? - Gibt es unbeabsichtigte Nebenwirkungen?

**Methoden:** - Follow-up-Audit - Stichproben - Monitoring - Interviews

**Dokumentation:** - Wirksamkeitsprüfung durchgeführt am - Methode - Ergebnis - Nachweis/Evidence

**Verantwortlich:** Auditor oder ISMS Manager

#### 16.2.7 2.7 Schritt 6: Abschluss

**Kriterien für Abschluss:** - Maßnahme vollständig umgesetzt - Wirksamkeit nachgewiesen - Dokumentation vollständig - Lessons Learned dokumentiert

- Abschluss-Aktivitäten:** - Finding-Status auf “Geschlossen” setzen - Dokumentation archivieren  
 - Stakeholder informieren - Lessons Learned kommunizieren

**Verantwortlich:** ISMS Manager

## 16.3 3. Nichtkonformitäten-Register

### 16.3.1 3.1 Aktive Nichtkonformitäten

Finding-ID	Quelle	Kategorie	Beschreibung	Root-Cause	Korrekturmaßnahmen	Owner	Fällig	Status	Wirksamkeit geprüft
F-2026-001	Audit	Minor	Dokumentation unvollständig	Prozess nicht definiert	[TODO] Dokumentieren	2026-03-31	In Arbeit	-	
F-2026-002	Incident	Major	Ungepatcht Schwachstelle ausgenutzt	Patch-Prozess unzureichend	Patch-Prozess verbessern	IT-Betrieb	2026-02-28	In Arbeit	-
F-2026-003	Monitoring	Observation	MFA-Aktivierung < 100%	MFA-Awareness unzureichend	Awareness-Kampagne	Thomas Weber	2026-04-30	Geplant	

[TODO: Aktive Nichtkonformitäten hinzufügen]

### 16.3.2 3.2 Geschlossene Nichtkonformitäten (Archiv)

Finding-ID	Quelle	Kategorie	Beschreibung	Korrekturmaßnahmen	Abschlussdatum	bestätigt	Wirksamkeit
F-2025-050	Audit	Minor	Backup-Tests nicht dokumentiert	Backup-Test-Prozess etabliert	2026-01-15	Ja	
F-2025-051	Incident	Major	Phishing-incident	Security Awareness Training	2026-01-20	Ja	

[TODO: Geschlossene Nichtkonformitäten archivieren]

## 16.4 4. Priorisierung und Fristen

### 16.4.1 4.1 Priorisierung

Kategorie	Priorität	Frist	Eskalation
Major Non-Conformity	Sehr hoch	30 Tage	Sofort an CISO und Geschäftsführung
Minor Non-Conformity Observation	Hoch Mittel	90 Tage 180 Tage	Bei Verzögerung an CISO Bei Verzögerung an ISMS Manager
Opportunity for Improvement	Niedrig	Nach Verfügbarkeit	Keine

## 16.4.2 4.2 Eskalation

**Überfällige Maßnahmen:** - > 2 Wochen überfällig: Erinnerung an Owner - > 4 Wochen überfällig: Eskalation an CISO - > 8 Wochen überfällig: Eskalation an Geschäftsführung

**Kritische Nichtkonformitäten:** - Major Non-Conformities: Sofortige Eskalation - Compliance-Verstöße: Sofortige Eskalation - Wiederholte Nichtkonformitäten: Eskalation an Management

## 16.5 5. Ursachenanalyse-Methoden

### 16.5.1 5.1 5-Why-Methode

**Beispiel:** 1. **Warum** trat die Nichtkonformität auf? → Ungepatchte Schwachstelle wurde ausgenutzt 2. **Warum** war die Schwachstelle ungepatcht? → Patch wurde nicht rechtzeitig installiert 3. **Warum** wurde der Patch nicht rechtzeitig installiert? → Patch-Prozess hat Patch nicht priorisiert 4. **Warum** hat der Prozess den Patch nicht priorisiert? → CVSS-Score wurde nicht berücksichtigt 5. **Warum** wurde CVSS-Score nicht berücksichtigt? → Prozess berücksichtigt nur Vendor-Severity

**Root Cause:** Patch-Priorisierung basiert nicht auf CVSS-Score

**Korrekturmaßnahme:** Patch-Prozess um CVSS-basierte Priorisierung erweitern

### 16.5.2 5.2 Fishbone-Diagramm (Ishikawa)

**Kategorien:** - **Mensch:** Fehlende Schulung, Fehler, Fahrlässigkeit - **Prozess:** Unzureichende Prozesse, fehlende Dokumentation - **Technologie:** Fehlende Tools, Fehlkonfiguration, Bugs - **Umgebung:** Organisatorische Faktoren, Ressourcenmangel

## 16.6 6. Wirksamkeitsprüfung

### 16.6.1 6.1 Methoden

**Audit:** - Follow-up-Audit - Stichprobenprüfung - Dokumentenprüfung

**Monitoring:** - KPI-Tracking - Incident-Tracking - Compliance-Monitoring

**Testing:** - Penetration Tests - Vulnerability Scans - Configuration Audits

**Interviews:** - Befragung betroffener Personen - Feedback-Sammlung

## 16.6.2 6.2 Erfolgskriterien

**Maßnahme ist wirksam, wenn:** - Nichtkonformität tritt nicht mehr auf - Root Cause ist beseitigt  
- KPIs haben sich verbessert - Keine neuen Probleme entstanden sind - Stakeholder sind zufrieden

## 16.7 7. Lessons Learned

### 16.7.1 7.1 Dokumentation

**Für jede geschlossene Nichtkonformität:** - Was haben wir gelernt? - Was hat gut funktioniert?  
- Was könnte verbessert werden? - Welche Maßnahmen sind übertragbar?

### 16.7.2 7.2 Kommunikation

**Zielgruppen:** - Betroffene Teams - ISMS-Gremium - Management - Alle Mitarbeiter (bei relevanten Lessons Learned)

**Kanäle:** - Lessons-Learned-Datenbank - Security Newsletter - Team-Meetings - Awareness-Kampagnen

## 16.8 8. Rollen und Verantwortlichkeiten

### 16.8.1 8.1 RACI-Matrix: Nichtkonformitäten-Prozess

Aktivität	CISO	ISMS Manager	Finding-Owner	Auditor	Geschäftsführung
Nichtkonformität erfassen	R		C	R	I
Ursachenanalyse	C		R	C	I
Maßnahme definieren	A	C	R	C	I
Maßnahme genehmigen	A	C	I	I	C
Maßnahme umsetzen	A	C	R	I	I
Wirksamkeit prüfen	A	R	C	R	I
Finding schließen	A	R	C	C	I

**Legende:** R = Responsible, A = Accountable, C = Consulted, I = Informed

## 16.9 9. Metriken und Reporting

### 16.9.1 9.1 KPIs

Metrik	Zielwert	Aktuell	Status
Offene Major Findings	0	[TODO]	/
Offene Minor Findings	< 5	[TODO]	/
Durchschnittliche Behebungszzeit (Major)	< 30 Tage	[TODO] Tage	/
Durchschnittliche Behebungszzeit (Minor)	< 90 Tage	[TODO] Tage	/
Überfällige Findings	0	[TODO]	/
Wiederkehrende Findings	0	[TODO]	/

### 16.9.2 9.2 Reporting

**Monatlich:** - Status aller offenen Findings - Überfällige Findings - Neu hinzugekommene Findings

**Quartalsweise:** - Trend-Analyse - Häufigste Ursachen - Wirksamkeit von Maßnahmen

**Jährlich:** - Vollständiger Review im Management Review - Lessons Learned Zusammenfassung

## 16.10 10. Referenzen

### 16.10.1 10.1 Interne Dokumente

- 0130\_ISMS\_Internes\_Auditprogramm.md - Internal Audit Program
- 0140\_ISMS\_Management\_Review\_Template.md - Management Review
- 0160\_ISMS\_Kontinuierliche\_Verbesserung.md - Continuous Improvement
- 0400\_Policy\_Incident\_Management.md - Incident Management

### 16.10.2 10.2 Externe Standards

- ISO/IEC 27001:2022 - Clause 10.1: Nonconformity and corrective action
- ISO 9001:2015 - Clause 10.2: Nonconformity and corrective action
- ISO 19011:2018 - Guidelines for auditing management systems

---

#### Genehmigt durch:

Thomas Weber, CISO

Datum: {{ meta.document.approval\_date }}

Nächster Review: {{ meta.document.next\_review }}

ewpage

# Chapter 17

## Kontinuierliche Verbesserung (KVP) im ISMS

**Dokument-ID:** 0160

**Dokumenttyp:** ISMS-Grundlagendokument

**Standard-Referenz:** ISO/IEC 27001:2022 Clause 10.2

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 17.1 1. Zweck und Ziele

#### 17.1.1 1.1 Zweck

Das Programm zur kontinuierlichen Verbesserung (KVP) der **AdminSend GmbH** stellt sicher, dass:

- Das ISMS kontinuierlich verbessert wird
- Verbesserungspotenziale systematisch identifiziert werden
- Verbesserungsmaßnahmen priorisiert und umgesetzt werden
- Die Eignung, Angemessenheit und Wirksamkeit des ISMS erhalten bleibt

#### 17.1.2 1.2 Ziele

- **Kontinuierliche Verbesserung:** Mindestens 10 Verbesserungsmaßnahmen pro Jahr
- **Lessons Learned:** Systematische Auswertung aller Incidents und Audits
- **Innovation:** Einsatz neuer Technologien und Best Practices
- **Effizienz:** Optimierung von Prozessen und Controls

#### 17.1.3 1.3 PDCA-Zyklus

Das ISMS folgt dem PDCA-Zyklus (Plan-Do-Check-Act):

## PDCA-Zyklus

### Plan (Planen)

- Ziele setzen
- Risiken analysieren
- Maßnahmen planen
- Ressourcen zuweisen

### Do (Umsetzen)

- Maßnahmen implementieren
- Schulungen durchführen
- Controls betreiben
- Dokumentieren

### Check (Überprüfen)

- Monitoring
- Audits
- Reviews
- KPIs messen

### Act (Handeln)

- Nichtkonformitäten beheben
- Verbesserungen umsetzen
- Lessons Learned
- Anpassungen vornehmen

[Zurück zu Plan \(Kontinuierlicher Zyklus\)](#)

## 17.2 2. Quellen für Verbesserungen

### 17.2.1 2.1 Audits und Findings

**Interne Audits:** - Audit-Findings (Major/Minor/Observations) - Opportunities for Improvement  
- Best Practices aus anderen Bereichen

**Externe Audits:** - Zertifizierungsaudits - Kundenaudits - Regulatorische Audits

**Siehe:** 0130\_ISMS\_Internes\_Auditprogramm.md

### 17.2.2 2.2 Incidents und Postmortems

**Security Incidents:** - Root Cause Analysis - Lessons Learned - Präventivmaßnahmen

**Near Misses:** - Beinahe-Vorfälle - Frühwarnindikatoren - Proaktive Maßnahmen

**Siehe:** 0400\_Policy\_Incident\_Management.md

### 17.2.3 2.3 Risikobewertungen

**Risikoanalyse:** - Neue Risiken - Geänderte Risikobewertungen - Emerging Threats

**Risikobehandlung:** - Wirksamkeit von Maßnahmen - Neue Behandlungsoptionen - Optimierungspotenziale

**Siehe:** 0080\_ISMS\_Risikoregister\_Template.md

### 17.2.4 2.4 KPIs und Monitoring

**Performance-Metriken:** - KPI-Trends - Abweichungen von Zielwerten - Benchmarking

**Monitoring-Daten:** - SIEM-Alerts - Vulnerability Scans - Log-Analysen

**Siehe:** 0110\_ISMS\_Sicherheitsziele\_und\_Metriken.md

### 17.2.5 2.5 Änderungen im Kontext

**Externe Änderungen:** - Neue Bedrohungen - Neue Technologien - Neue Regulierungen - Branchentrends

**Interne Änderungen:** - Organisatorische Änderungen - Neue Systeme/Prozesse - Strategische Ausrichtung

**Siehe:** 0030\_ISMS\_Kontext\_und\_Interessierte\_Parteien.md

### 17.2.6 2.6 Stakeholder-Feedback

**Kunden:** - Sicherheitsanforderungen - Zufriedenheitsumfragen - Beschwerden

**Mitarbeiter:** - Feedback zu Prozessen - Verbesserungsvorschläge - Usability-Probleme

**Management:** - Strategische Vorgaben - Ressourcen-Entscheidungen

### 17.2.7 2.7 Best Practices und Innovation

**Externe Quellen:** - Branchenstandards (NIST, CIS, etc.) - Security-Konferenzen - Threat Intelligence - Peer-Austausch

**Interne Innovation:** - Proof of Concepts - Pilotprojekte - Technologie-Evaluierungen

## 17.3 3. KVP-Backlog

### 17.3.1 3.1 Verbesserungsvorschläge

Item-ID	Titel	Quelle	Beschreibung	Nutzen	Aufwand	Owner	Priorität	Status
KVP-001	SIEM-Automatisierung	Monitoring Automatische Response-Playbooks	Schnellere Incident-Response	40 PT	Security Team	Hoch	Geplant	
KVP-002	Zero-Trust-Architektur	Best Practice Segmentation	Implementierung Zero-Trust-Prinzipien	Verbessert Segmentation	200 PT	Anna Schmidt	Mittel	Evaluierung
KVP-003	Security Awareness	Champions in allen Teams	Awareness Multiplikatoren	Höheres Security Awareness	20 PT	Thomas Weber	Hoch	In Arbeit
KVP-004	Immutability	DevOps Infrastruktur	Infrastructure as Code mit Immutability	Bessere Compliance, weniger Drift	80 PT	DevOps	Mittel	Geplant

[TODO: Weitere Verbesserungsvorschläge hinzufügen]

### 17.3.2 3.2 Priorisierung

**Priorisierungskriterien:**

Kriterium	Gewichtung	Bewertung (1-5)
Risikoreduktion	40%	Wie stark wird Risiko reduziert?
Compliance-Nutzen	20%	Verbessert Compliance?
Effizienzgewinn	20%	Spart Zeit/Ressourcen?
Aufwand	10%	Wie hoch ist der Aufwand? (invertiert)
Strategische Ausrichtung	10%	Passt zur Strategie?

**Priorisierungsformel:**

$$\text{Priorität} = (\text{Risikoreduktion} \times 0,4) + (\text{Compliance} \times 0,2) + (\text{Effizienz} \times 0,2) + ((6 - \text{Aufwand}) \times 0,1) + (\text{Strategie} \times 0,1)$$

**Prioritätsstufen:** - Sehr hoch (4,0-5,0): Sofort umsetzen - Hoch (3,0-3,9): Innerhalb 6 Monate - Mittel (2,0-2,9): Innerhalb 12 Monate - Niedrig (< 2,0): Nach Verfügbarkeit

## 17.4 4. Verbesserungsprozess

### 17.4.1 4.1 Prozessschritte

#### 1. Identifikation

- Verbesserungspotenzial erkennen
- Beschreibung erstellen
- In Backlog aufnehmen

#### 2. Bewertung

- Nutzen bewerten
- Aufwand schätzen
- Priorisieren
- Genehmigung einholen

#### 3. Planung

- Detailplanung
- Ressourcen zuweisen
- Zeitplan erstellen
- Stakeholder informieren

#### 4. Umsetzung

- Implementierung
- Testing
- Dokumentation
- Schulung

#### 5. Review

- Wirksamkeit prüfen
- Lessons Learned
- Dokumentation
- Kommunikation

### 17.4.2 4.2 Genehmigungsprozess

**Kleine Verbesserungen (< 10 PT, < 5.000 €):** - Genehmigung durch CISO

**Mittlere Verbesserungen (10-40 PT, 5.000-25.000 €):** - Genehmigung durch CISO und CIO

**Große Verbesserungen (> 40 PT, > 25.000 €):** - Genehmigung durch Geschäftsführung - Präsentation im Informationssicherheitsgremium

## 17.5 5. Verbesserungskategorien

### 17.5.1 5.1 Prozessverbesserungen

**Ziel:** Effizienzsteigerung, Fehlerreduktion

**Beispiele:** - Automatisierung manueller Prozesse - Vereinfachung komplexer Prozesse - Integration von Tools - Standardisierung

## **17.5.2 5.2 Control-Verbesserungen**

**Ziel:** Erhöhung der Wirksamkeit

**Beispiele:** - Neue Security Controls - Verbesserung bestehender Controls - Automatisierung von Controls - Monitoring-Erweiterungen

## **17.5.3 5.3 Technologie-Verbesserungen**

**Ziel:** Modernisierung, Innovation

**Beispiele:** - Neue Security-Tools - Cloud-Migration - Zero-Trust-Architektur - KI/ML-basierte Security

## **17.5.4 5.4 Awareness-Verbesserungen**

**Ziel:** Erhöhung des Sicherheitsbewusstseins

**Beispiele:** - Neue Schulungsformate - Gamification - Security Champions - Awareness-Kampagnen

## **17.5.5 5.5 Dokumentations-Verbesserungen**

**Ziel:** Klarheit, Vollständigkeit

**Beispiele:** - Aktualisierung veralteter Dokumente - Neue Templates - Bessere Strukturierung - Automatisierte Dokumentation

# **17.6 6. Lessons Learned**

## **17.6.1 6.1 Lessons-Learned-Prozess**

**Nach jedem Incident/Audit/Projekt:** 1. Lessons-Learned-Session durchführen 2. Erkenntnisse dokumentieren 3. Verbesserungsmaßnahmen ableiten 4. In KVP-Backlog aufnehmen 5. Kommunizieren

## **17.6.2 6.2 Lessons-Learned-Datenbank**

**Struktur:** - Datum und Kontext - Was ist passiert? - Was haben wir gelernt? - Was hat gut funktioniert? - Was könnte verbessert werden? - Abgeleitete Maßnahmen - Status der Maßnahmen

**Zugriff:** - Alle Mitarbeiter (lesend) - ISMS-Team (schreibend)

## **17.6.3 6.3 Kommunikation**

**Zielgruppen:** - Betroffene Teams - ISMS-Gremium - Management - Alle Mitarbeiter (bei relevanten Lessons Learned)

**Kanäle:** - Lessons-Learned-Datenbank - Security Newsletter - Team-Meetings - Awareness-Kampagnen

## 17.7 7. Innovation und Best Practices

### 17.7.1 7.1 Technologie-Radar

**Beobachtung neuer Technologien:** - Emerging Security Technologies - Cloud Security - Zero Trust - AI/ML in Security - DevSecOps

**Bewertung:** - Adopt (Einsetzen) - Trial (Ausprobieren) - Assess (Bewerten) - Hold (Abwarten)

### 17.7.2 7.2 Proof of Concepts (PoCs)

**Prozess:** 1. Technologie identifizieren 2. PoC-Scope definieren 3. PoC durchführen 4. Evaluieren  
5. Entscheidung: Adopt / Reject

**Budget:** - Jährliches PoC-Budget: [TODO] €

### 17.7.3 7.3 Benchmarking

**Vergleich mit:** - Branchenstandards - Peer-Organisationen - Best Practices

**Quellen:** - NIST Cybersecurity Framework - CIS Controls - SANS Top 20 - Gartner/Forrester Reports

## 17.8 8. Metriken und Reporting

### 17.8.1 8.1 KVP-KPIs

Metrik	Zielwert	Aktuell	Status
Anzahl Verbesserungsmaßnahmen pro Jahr	10	[TODO]	/
Durchschnittliche Umsetzungszeit	< 90 Tage	[TODO] Tage	/
Umgesetzte Verbesserungen	80%	[TODO]%	/
Lessons Learned dokumentiert	100%	[TODO]%	/
PoCs durchgeführt	3 pro Jahr	[TODO]	/

### 17.8.2 8.2 Reporting

**Quartalsweise:** - Status KVP-Backlog - Umgesetzte Verbesserungen - Lessons Learned Zusammenfassung

**Jährlich:** - Vollständiger KVP-Bericht im Management Review - Trend-Analyse - Erfolgsgeschichten

## 17.9 9. Rollen und Verantwortlichkeiten

### 17.9.1 9.1 RACI-Matrix: Kontinuierliche Verbesserung

Aktivität	CISO	ISMS Manager	Verbesserungs-Owner	Teams	Geschäftsführung
Verbesserungen A identifizieren	R	R		R	I
Verbesserungen A bewerten	R	C		C	I
Verbesserungen A priorisieren	R	C		C	C
Verbesserungen A genehmigen	C	I		I	C
Verbesserungen A umsetzen	C	R		R	I
Wirksamkeit A prüfen	R	C		C	I
Lessons Learned dokumentieren	A	R	R	C	I

**Legende:** R = Responsible, A = Accountable, C = Consulted, I = Informed

## 17.10 10. Referenzen

### 17.10.1 10.1 Interne Dokumente

- 0110\_ISMS\_Sicherheitsziele\_und\_Metriken.md - Security Objectives
- 0130\_ISMS\_Internes\_Auditprogramm.md - Internal Audit Program
- 0140\_ISMS\_Management\_Review\_Template.md - Management Review
- 0150\_ISMS\_Nichtkonformitaeten\_und\_Korrekturmaßnahmen.md - Non-conformities
- 0400\_Policy\_Incident\_Management.md - Incident Management

### 17.10.2 10.2 Externe Standards

- ISO/IEC 27001:2022 - Clause 10.2: Continual improvement
- ISO 9001:2015 - Clause 10.3: Continual improvement
- NIST Cybersecurity Framework - Continuous improvement practices

---

#### Genehmigt durch:

Thomas Weber, CISO

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 18

## Policy: Akzeptable Nutzung IT

**Dokument-ID:** 0200

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.10 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 18.1 1. Zweck

Diese Policy definiert die Grundsätze für die akzeptable Nutzung von IT-Ressourcen der **AdminSend GmbH**. Sie stellt sicher, dass IT-Systeme, Anwendungen und Informationen ausschließlich für geschäftliche Zwecke und in Übereinstimmung mit gesetzlichen und regulatorischen Anforderungen genutzt werden.

### 18.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Systeme:** Alle IT-Systeme, Netzwerke, Anwendungen, E-Mail, Internet, Cloud-Services
- **Personen:** Alle Mitarbeiter, Auftragnehmer, Zeitarbeiter, Praktikanten und Dritte mit Zugang zu IT-Ressourcen
- **Geräte:** Unternehmenseigene und private Geräte (BYOD), die auf Unternehmensressourcen zugreifen
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_) zulässig.

## **18.3 3. Grundsätze (Policy Statements)**

### **18.3.1 3.1 Geschäftliche Nutzung**

IT-Ressourcen der Organisation werden primär für geschäftliche Zwecke bereitgestellt. Private Nutzung ist nur in dem Maße gestattet, wie sie die geschäftliche Nutzung nicht beeinträchtigt und den Sicherheitsrichtlinien entspricht.

### **18.3.2 3.2 Verantwortungsvolle Nutzung**

Nutzer sind verpflichtet, IT-Ressourcen verantwortungsvoll, effizient und in Übereinstimmung mit allen geltenden Richtlinien zu nutzen. Missbrauch, Verschwendungen oder Beschädigung von IT-Ressourcen ist untersagt.

### **18.3.3 3.3 Verbote Aktivitäten**

Folgende Aktivitäten sind ausdrücklich untersagt: - Zugriff auf, Speicherung oder Verbreitung illegaler, beleidigender oder unangemessener Inhalte - Umgehung von Sicherheitskontrollen oder unbefugter Zugriff auf Systeme - Installation nicht genehmigter Software oder Änderung von Systemkonfigurationen - Nutzung von IT-Ressourcen für kommerzielle Zwecke außerhalb der Geschäftstätigkeit - Versand von Spam, Phishing oder anderen schädlichen Kommunikationen

### **18.3.4 3.4 Datenschutz und Vertraulichkeit**

Nutzer müssen die Vertraulichkeit von Unternehmensinformationen wahren und dürfen keine vertraulichen Informationen ohne Genehmigung weitergeben oder veröffentlichen.

### **18.3.5 3.5 Monitoring und Überwachung**

Die Organisation behält sich das Recht vor, die Nutzung von IT-Ressourcen zu überwachen, um Sicherheit, Compliance und ordnungsgemäße Nutzung sicherzustellen. Nutzer haben keine Erwartung an Privatsphäre bei der Nutzung von Unternehmensressourcen.

### **18.3.6 3.6 Persönliche Verantwortung**

Nutzer sind persönlich verantwortlich für alle Aktivitäten, die unter ihren Zugangsdaten durchgeführt werden. Zugangsdaten dürfen nicht weitergegeben werden.

## **18.4 4. Rollen und Verantwortlichkeiten**

### **18.4.1 RACI-Matrix: Akzeptable Nutzung IT**

Aktivität	CISO	IT-Betrieb	HR	Mitarbeiter	Legal/Compliance
Policy-Erstellung	R/A	C	C	I	C
Policy-Kommunikation	R	C	R	I	I
Schulung und Awareness	C	C	R	R	I
Monitoring und Überwachung	A	R	I	I	C
Verstöße untersuchen	R	C	R	I	C
Sanktionen durchsetzen	C	I	R/A	I	C

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

#### 18.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **Umsetzungsverantwortliche:** IT-Betrieb, HR
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit, Legal/Compliance

### 18.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

#### 18.5.1 Zugehörige Richtlinien

- **0210\_Richtlinie\_Akzeptable\_Nutzung\_IT.md** - Detaillierte Implementierungsrichtlinie
- **0220\_Policy\_Zugriffssteuerung\_und\_Identitätsmanagement.md** - Access Control Policy
- **0500\_Policy\_Mobile\_Device\_und\_Remote\_Work.md** - Mobile Device Policy
- **0660\_Policy\_Informationsübertragung\_und\_Kommunikation.md** - Communication Policy

#### 18.5.2 Zugehörige Standards/Baselinses

- E-Mail-Nutzungsrichtlinie
- Internet-Nutzungsrichtlinie
- BYOD-Richtlinie (Bring Your Own Device)
- Social Media Guidelines

#### 18.5.3 Zugehörige Prozesse

- User Onboarding/Offboarding
- Incident Response bei Policy-Verstößen
- HR-Disziplinarverfahren

### 18.6 6. Compliance, Monitoring und Durchsetzung

#### 18.6.1 Messgrößen und KPIs

- Anzahl Policy-Verstöße pro Quartal
- Schulungsteilnahme-Quote (Ziel: 100% jährlich)
- Anzahl blockierter unangemessener Zugriffe
- Durchschnittliche Zeit zur Untersuchung von Verstößen
- Wiederholungstäter-Rate

#### 18.6.2 Nachweise und Evidence

- Schulungsnachweise und Bestätigungen
- Monitoring-Logs und Audit-Trails
- Incident-Reports bei Verstößen
- Disziplinarmaßnahmen-Dokumentation

- Awareness-Kampagnen-Metriken

### 18.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:

- **Leichte Verstöße:** Verwarnung, Nachschulung, Monitoring - **Mittlere Verstöße:** Schriftliche Abmahnung, temporäre Zugriffsbeschränkungen - **Schwere Verstöße:** Arbeitsrechtliche Konsequenzen bis zur Kündigung, rechtliche Schritte - **Vorsätzliche Verstöße:** Sofortige Sperrung, Kündigung, Strafanzeige

## 18.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und ggf. HR genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden dokumentiert und regelmäßig überprüft
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet

## 18.8 8. Referenzen

### 18.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0210\_Richtlinie\_Akzeptable\_Nutzung\_IT.md - Detailed Guideline
- 0400\_Policy\_Incident\_Management.md - Incident Management Policy
- 0530\_Richtlinie\_HR\_Onboarding\_Rollenwechsel\_Offboarding.md - HR Security Guideline

### 18.8.2 Externe Standards und Vorgaben

- **ISO/IEC 27001:2022 Annex A.5.10** - Acceptable use of information and other associated assets
- **ISO/IEC 27002:2022** - Information security controls
- **DSGVO (EU 2016/679)** - Datenschutz-Grundverordnung
- Arbeitsrechtliche Vorgaben zur IT-Nutzung

#### Genehmigt durch:

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 19

## Richtlinie: Akzeptable Nutzung IT

**Dokument-ID:** 0210

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0200\_Policy\_Akzeptable\_Nutzung\_IT.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.10

**Owner:** {{ meta.it\_operations.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 19.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0200\_Policy\_Akzeptable\_Nutzung\_IT.md und definiert detaillierte Regeln, Verfahren und technische Kontrollen für die akzeptable Nutzung von IT-Ressourcen bei **AdminSend GmbH**.

**Geltungsbereich:** - Alle Mitarbeiter, Auftragnehmer und Dritte mit Zugang zu IT-Ressourcen - Alle IT-Systeme, Netzwerke, Anwendungen und Geräte - Standorte: {{ netbox.site.name }} und alle Betriebsstandorte

### 19.2 2. Detaillierte Nutzungsregeln

#### 19.2.1 2.1 E-Mail-Nutzung

**Erlaubte Nutzung:** - Geschäftliche Kommunikation mit Kunden, Partnern und Kollegen - Begrenzte private Nutzung (max. 10 E-Mails pro Tag, keine großen Anhänge) - Anmeldung bei geschäftlichen Online-Diensten

**Verbotene Aktivitäten:** - Versand von Spam, Kettenmails oder unerwünschten Massenmails - Versand vertraulicher Informationen ohne Verschlüsselung - Nutzung privater E-Mail-Konten für

geschäftliche Kommunikation - Öffnen verdächtiger Anhänge oder Links (siehe Phishing-Awareness)  
- Automatische Weiterleitung geschäftlicher E-Mails an externe Adressen

**Technische Kontrollen:** - E-Mail-Filtering und Anti-Spam-Systeme - DLP (Data Loss Prevention) für ausgehende E-Mails - E-Mail-Archivierung für Compliance (Aufbewahrung: {{ meta.retention.email\_years }} Jahre) - Verschlüsselung für vertrauliche E-Mails (S/MIME oder PGP)

### 19.2.2 2.2 Internet-Nutzung

**Erlaubte Nutzung:** - Recherche für geschäftliche Zwecke - Zugriff auf genehmigte Cloud-Services und SaaS-Anwendungen - Begrenzte private Nutzung in Pausen (max. 30 Minuten pro Tag) - Zugriff auf Fachportale, Dokumentationen und Schulungsressourcen

**Verbotene Aktivitäten:** - Zugriff auf illegale, pornografische oder gewaltverherrlichende Inhalte - Download nicht genehmigter Software oder Dateien - Streaming von Videos/Musik während der Arbeitszeit (außer geschäftlich) - Nutzung von Anonymisierungsdiensten (VPN, Proxy) ohne Genehmigung - Online-Shopping, Glücksspiel oder private Geschäftstätigkeiten

**Technische Kontrollen:** - Web-Filtering und URL-Kategorisierung - Blockierung bekannter Malware- und Phishing-Sites - Bandbreitenmanagement für Streaming-Dienste - Logging und Monitoring der Internet-Nutzung - SSL-Inspection für verschlüsselten Traffic (mit Datenschutz-Compliance)

### 19.2.3 2.3 Software-Installation und -Nutzung

**Erlaubte Aktivitäten:** - Nutzung genehmigter Software aus dem Software-Katalog - Installation von Software durch IT-Betrieb oder über Self-Service-Portal - Nutzung von Browser-Extensions aus genehmigter Whitelist

**Verbotene Aktivitäten:** - Installation nicht genehmigter Software (Shadow IT) - Nutzung von Raubkopien oder unlizenzierte Software - Installation von Peer-to-Peer-Software (Torrents, File-Sharing) - Deaktivierung oder Umgehung von Sicherheitssoftware (Antivirus, EDR) - Änderung von Systemkonfigurationen ohne Genehmigung

**Technische Kontrollen:** - Application Whitelisting (nur genehmigte Software kann ausgeführt werden) - Software Asset Management (SAM) für Lizenz-Compliance - Endpoint Protection (Antivirus, EDR) mit Tamper Protection - Regelmäßige Software-Inventarisierung - Patch Management für genehmigte Software

### 19.2.4 2.4 Datenhandling und Speicherung

**Erlaubte Aktivitäten:** - Speicherung geschäftlicher Daten auf genehmigten Netzlaufwerken und Cloud-Speichern - Nutzung von {{ meta.cloud.storage\_service }} für Dateiablage - Verschlüsselung vertraulicher Daten gemäß Klassifizierung

**Verbotene Aktivitäten:** - Speicherung geschäftlicher Daten auf privaten Cloud-Diensten (Dropbox, Google Drive privat) - Speicherung vertraulicher Daten auf lokalen Festplatten ohne Verschlüsselung - Weitergabe von Zugangsdaten oder Passwörtern - Exfiltration großer Datenmengen ohne Genehmigung

**Technische Kontrollen:** - DLP (Data Loss Prevention) für Datentransfer-Überwachung - Verschlüsselung von Festplatten (BitLocker, FileVault) - Cloud Access Security Broker (CASB) für Cloud-Service-Überwachung - Netzwerk-Segmentierung für sensible Daten - Backup und Retention gemäß 0420\_Policy\_Backup\_und\_Wiederherstellung.md

### 19.2.5 2.5 Mobile Geräte und BYOD

**Erlaubte Aktivitäten:** - Nutzung unternehmenseigener Mobilgeräte für geschäftliche Zwecke - BYOD (Bring Your Own Device) nach Registrierung und MDM-Enrollment - Zugriff auf genehmigte Unternehmensanwendungen über Mobile Apps

**Verbotene Aktivitäten:** - Jailbreak oder Rooting von Geräten - Installation nicht genehmigter Apps auf BYOD-Geräten mit Unternehmenszugriff - Speicherung vertraulicher Daten auf privaten Geräten ohne Container - Nutzung unsicherer WLAN-Netzwerke ohne VPN

**Technische Kontrollen:** - Mobile Device Management (MDM) für alle Geräte mit Unternehmenszugriff - Containerisierung für geschäftliche Daten auf BYOD-Geräten - Remote Wipe bei Verlust oder Diebstahl - Erzwungene Verschlüsselung und PIN/Biometrie - Compliance-Checks (OS-Version, Jailbreak-Detection)

**Details:** Siehe 0500\_Policy\_Mobile\_Device\_und\_Remote\_Work.md

### 19.2.6 2.6 Social Media und externe Kommunikation

**Erlaubte Aktivitäten:** - Nutzung von Social Media für Marketing und Unternehmenskommunikation (autorisierte Accounts) - Professionelle Nutzung von LinkedIn, Xing für Networking - Teilnahme an Fachforen und Communities (mit Disclaimer)

**Verbotene Aktivitäten:** - Veröffentlichung vertraulicher Unternehmensinformationen - Negative Äußerungen über Unternehmen, Kunden oder Kollegen - Vortäuschen einer offiziellen Unternehmensmeinung ohne Autorisierung - Nutzung von Unternehmenslogos ohne Genehmigung

**Richtlinien:** - Social Media Guidelines für Mitarbeiter - Genehmigungsprozess für offizielle Unternehmens-Accounts - Schulung zu Social Engineering und Phishing über Social Media

### 19.2.7 2.7 Remote Work und VPN-Nutzung

**Erlaubte Aktivitäten:** - Remote-Zugriff über genehmigte VPN-Verbindungen - Nutzung von Remote Desktop (RDP, Citrix) für Systemzugriff - Arbeit von Home Office nach Genehmigung

**Verbotene Aktivitäten:** - Nutzung unsicherer Netzwerke ohne VPN - Weitergabe von VPN-Zugangsdaten - Arbeit in öffentlichen Bereichen mit Einsicht auf Bildschirm (Shoulder Surfing) - Nutzung privater Geräte ohne MDM-Enrollment

**Technische Kontrollen:** - VPN mit Multi-Faktor-Authentifizierung (MFA) - Zero Trust Network Access (ZTNA) für granulare Zugriffskontrolle - Endpoint Compliance Checks vor VPN-Zugriff - Session-Timeouts und Idle-Disconnects

**Details:** Siehe 0500\_Policy\_Mobile\_Device\_und\_Remote\_Work.md

## 19.3 3. Monitoring und Überwachung

### 19.3.1 3.1 Monitoring-Umfang

Die Organisation überwacht folgende Aktivitäten zur Sicherstellung von Sicherheit und Compliance:

- **E-Mail-Verkehr:** Metadaten (Absender, Empfänger, Betreff), DLP-Scans
- **Internet-Nutzung:** Besuchte URLs, Kategorien, Bandbreitennutzung
- **Dateitransfers:** Uploads/Downloads, Cloud-Service-Nutzung
- **Systemzugriffe:** Login-Aktivitäten, privilegierte Zugriffe
- **Anwendungsnutzung:** Genutzte Anwendungen, Nutzungsdauer

### 19.3.2 3.2 Datenschutz und Privatsphäre

**Grundsätze:** - Monitoring erfolgt zweckgebunden für Sicherheit und Compliance - Keine anlasslose Überwachung individueller Mitarbeiter - Monitoring-Daten werden nur bei begründetem Verdacht analysiert - Einhaltung der DSGVO und Betriebsvereinbarungen

**Transparenz:** - Mitarbeiter werden über Monitoring-Maßnahmen informiert (Onboarding, Schulungen) - Betriebsrat wird bei Monitoring-Maßnahmen einbezogen - Datenschutzbeauftragter prüft Monitoring-Konzepte

### 19.3.3 3.3 Incident Response bei Verstößen

**Prozess:** 1. **Detektion:** Automatische Alerts bei Policy-Verstößen (DLP, Web-Filter, SIEM)

**Triage:** IT-Security prüft Alert und bewertet Schweregrad 3. **Untersuchung:** Bei begründetem Verdacht: Detaillierte Analyse, Einbeziehung HR 4. **Maßnahmen:** Je nach Schweregrad: Verwarnung, Schulung, Disziplinarmaßnahmen 5. **Dokumentation:** Incident-Report, Lessons Learned

**Eskalation:** - Leichte Verstöße: IT-Betrieb informiert Vorgesetzten - Mittlere Verstöße: CISO und HR werden einbezogen - Schweren Verstöße: Geschäftsführung, Legal, ggf. Strafverfolgung

## 19.4 4. Schulung und Awareness

### 19.4.1 4.1 Pflichtschulungen

**Onboarding:** - Acceptable Use Policy Training (1 Stunde) - Phishing-Awareness-Training - Datenschutz-Grundlagen

**Jährliche Auffrischung:** - Acceptable Use Policy Refresher (30 Minuten) - Aktuelle Bedrohungen und Best Practices - Quiz zur Wissensüberprüfung (Bestehensgrenze: 80%)

### 19.4.2 4.2 Awareness-Kampagnen

**Regelmäßige Maßnahmen:** - Monatliche Security-Newsletter - Phishing-Simulationen (quartalsweise) - Poster und Infografiken zu Sicherheitsthemen - Lunch & Learn Sessions zu aktuellen Themen

### 19.4.3 4.3 Dokumentation

**Nachweise:** - Schulungsteilnahme-Tracking in LMS (Learning Management System) - Bestätigungen der Policy-Kenntnisnahme (jährlich) - Quiz-Ergebnisse und Zertifikate - Phishing-Simulation-

## Ergebnisse

# 19.5 5. Ausnahmen und Sonderfälle

## 19.5.1 5.1 Ausnahmenprozess

**Antrag:** - Formular: Ausnahmeantrag mit Begründung und Risikobewertung - Genehmigung: CISO (bei technischen Ausnahmen), HR (bei Nutzungsausnahmen) - Befristung: Max. 12 Monate, danach erneute Prüfung

**Beispiele für Ausnahmen:** - Installation spezieller Software für Projekte - Erweiterte Internet-Zugriffe für Forschung - Nutzung privater Geräte ohne MDM (temporär)

**Dokumentation:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md

## 19.5.2 5.2 Privilegierte Nutzer

**Administratoren und IT-Betrieb:** - Erweiterte Rechte für Systemadministration - Zusätzliche Schulungen und Background Checks - Erhöhtes Monitoring privilegierter Aktivitäten - Vier-Augen-Prinzip bei kritischen Änderungen

**Details:** Siehe 0230\_Richtlinie\_IAM\_Joiner\_Mover\_Leaver\_und\_Zugriffsantraege.md

# 19.6 6. Technische Implementierung

## 19.6.1 6.1 Technologie-Stack

**Sicherheitstools:** - **Web-Filter:** {{ meta.security.web\_filter }} (z.B. Cisco Umbrella, Zscaler) - **E-Mail-Security:** {{ meta.security.email\_gateway }} (z.B. Proofpoint, Mimecast) - **DLP:** {{ meta.security.dlp\_solution }} (z.B. Microsoft Purview, Symantec DLP) - **Endpoint Protection:** {{ meta.security.edr\_solution }} (z.B. CrowdStrike, SentinelOne) - **CASB:** {{ meta.security.casb\_solution }} (z.B. Microsoft Defender for Cloud Apps)

**Monitoring und Logging:** - **SIEM:** {{ meta.security.siem\_solution }} (z.B. Splunk, Microsoft Sentinel) - **Log-Retention:** {{ meta.retention.log\_years }} Jahre für Security-Logs - **Alerting:** Automatische Alerts bei kritischen Verstößen

## 19.6.2 6.2 Konfigurationsbeispiele

**Web-Filter-Kategorien (blockiert):** - Adult Content, Gambling, Illegal Drugs - Malware, Phishing, Command & Control - Anonymizers, Proxy Avoidance - Peer-to-Peer, File Sharing (außer genehmigte Dienste)

**DLP-Regeln:** - Blockierung von Kreditkartennummern in E-Mails - Warnung bei Versand von Dokumenten mit "Vertraulich"-Klassifizierung - Blockierung von Uploads zu nicht genehmigten Cloud-Diensten - Erkennung von PII (Personally Identifiable Information) in Dateitransfers

**Application Whitelisting:** - Nur signierte Anwendungen aus genehmigtem Katalog - Blockierung von PowerShell/CMD für Standard-Nutzer - Ausnahmen für Entwickler und Administratoren

## 19.7 7. Compliance und Audit

### 19.7.1 7.1 Messgrößen (KPIs)

Metrik	Zielwert	Messung
Schulungsteilnahme	100% jährlich	LMS-Reports
Policy-Verstöße	< 5 pro Monat	SIEM-Alerts
Phishing-Klickrate	< 5%	Simulation-Ergebnisse
Nicht genehmigte Software	0 Installationen	Software-Inventar
DLP-Incidents	< 10 pro Monat	DLP-Reports

### 19.7.2 7.2 Audit-Nachweise

**Dokumentation:** - Policy-Dokumente und Versionshistorie - Schulungsnachweise und Bestätigungen - Monitoring-Logs und Incident-Reports - Ausnahmen-Register - Audit-Trails für Zugriffe und Änderungen

**Audit-Frequenz:** - Interne Audits: Jährlich - Externe Audits: Bei ISO 27001-Zertifizierung - Ad-hoc-Audits: Bei Verdacht auf Verstöße

## 19.8 8. Review und Aktualisierung

**Review-Zyklus:** - Jährlicher Review durch CISO und IT-Betrieb - Ad-hoc-Updates bei neuen Bedrohungen oder Technologien - Einbeziehung von HR und Legal bei Änderungen

**Change Management:** - Änderungen werden über Change-Prozess gesteuert - Kommunikation an alle Mitarbeiter bei wesentlichen Änderungen - Aktualisierung von Schulungsmaterialien

## 19.9 9. Referenzen

### 19.9.1 Interne Dokumente

- 0200\_Policy\_Akzeptable\_Nutzung\_IT.md - Übergeordnete Policy
- 0220\_Policy\_Zugriffssteuerung\_und\_Identitätsmanagement.md - Access Control
- 0320\_PolicyLogging\_und\_Monitoring.md - Logging Policy
- 0400\_Policy\_Incident\_Management.md - Incident Management
- 0500\_Policy\_Mobile\_Device\_und\_Remote\_Work.md - Mobile Device Policy
- 0640\_Policy\_Ausnahmen\_und\_Risk\_Wavers.md - Exception Process

### 19.9.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.5.10 - Acceptable use of information
- ISO/IEC 27002:2022 - Information security controls
- DSGVO (EU 2016/679) - Datenschutz-Grundverordnung
- Betriebsverfassungsgesetz (BetrVG) - Mitbestimmung bei Monitoring

**Genehmigt durch:**

Thomas Weber, CISO

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 20

## Policy: Zugriffssteuerung und Identitätsmanagement

**Dokument-ID:** 0220

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.15-A.5.18 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 20.1 1. Zweck

Diese Policy definiert die Grundsätze für Zugriffssteuerung und Identitätsmanagement (IAM) der **AdminSend GmbH**. Sie stellt sicher, dass der Zugriff auf Informationen und IT-Systeme ausschließlich autorisierten Personen gewährt wird und auf Basis des Need-to-Know-Prinzips und der geringsten Privilegien (Least Privilege) erfolgt.

### 20.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Systeme:** Alle IT-Systeme, Anwendungen, Datenbanken, Netzwerke, Cloud-Services
- **Personen:** Alle Mitarbeiter, Auftragnehmer, Lieferanten und Dritte mit Zugang zu IT-Ressourcen
- **Zugriffsmethoden:** Lokaler Zugriff, Remote-Zugriff, privilegierter Zugriff, API-Zugriff
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_) zulässig.

## 20.3 3. Grundsätze (Policy Statements)

### 20.3.1 3.1 Least Privilege (Geringste Privilegien)

Nutzer erhalten nur die minimalen Zugriffsrechte, die zur Erfüllung ihrer Aufgaben erforderlich sind. Privilegierte Zugriffe werden restriktiv vergeben und regelmäßig überprüft.

### 20.3.2 3.2 Need-to-Know-Prinzip

Der Zugriff auf Informationen wird nur gewährt, wenn eine geschäftliche Notwendigkeit besteht. Zugriffe werden auf Basis von Rollen und Verantwortlichkeiten vergeben.

### 20.3.3 3.3 Identitätslebenszyklus (Joiner-Mover-Leaver)

Identitäten werden über den gesamten Lebenszyklus verwaltet: - **Joiner:** Zugriffsrechte werden bei Eintritt basierend auf Rolle und Funktion vergeben - **Mover:** Zugriffsrechte werden bei Rollenwechsel angepasst (alte Rechte entziehen, neue gewähren) - **Leaver:** Alle Zugriffsrechte werden bei Austritt unverzüglich entzogen

### 20.3.4 3.4 Rollenbasierte Zugriffskontrolle (RBAC)

Zugriffsrechte werden primär über Rollen und Gruppen vergeben, nicht über individuelle Berechtigungen. Rollenmodelle werden regelmäßig überprüft und aktualisiert.

### 20.3.5 3.5 Segregation of Duties (Funktionstrennung)

Kritische Funktionen werden so aufgeteilt, dass keine einzelne Person alle Schritte eines sensiblen Prozesses durchführen kann. Dies verhindert Betrug und Fehler.

### 20.3.6 3.6 Regelmäßige Rezertifizierung

Zugriffsrechte werden regelmäßig (mindestens jährlich) überprüft und rezertifiziert. Nicht mehr benötigte Rechte werden entzogen.

### 20.3.7 3.7 Privileged Access Management (PAM)

Privilegierte Accounts (Administratoren, Root, Service-Accounts) unterliegen besonderen Kontrollen: - Separate Accounts für privilegierte Tätigkeiten - Just-in-Time (JIT) Access wo möglich - Umfassende Protokollierung und Überwachung

### 20.3.8 3.8 Zugriffsgenehmigung und Dokumentation

Alle Zugriffsvergaben müssen durch den Ressourcen-Owner genehmigt und dokumentiert werden. Zugriffsentscheidungen sind nachvollziehbar und auditierbar.

## 20.4 4. Rollen und Verantwortlichkeiten

### 20.4.1 RACI-Matrix: Zugriffssteuerung und IAM

Aktivität	CISO	IT-Betrieb	Ressourcen-Owner	HR	Mitarbeiter
Policy-Erstellung	R/A	C	C	C	I
IAM-System-Betrieb	C	R/A	I	I	I
Zugriff beantragen	I	I	C	I	R
Zugriff genehmigen	C	I	R/A	C	I
Zugriff provisionieren	I	R	I	I	I
Rezertifizierung	C	C	R/A	C	I
Zugriff entziehen (Leaver)	C	R	I	R/A	I
Monitoring und Audits	R/A	C	C	I	I

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

#### 20.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **IAM-Verantwortlicher:** {{ meta.it.iam\_manager }}
- **Ressourcen-Owner:** Fachbereichsleiter, Systemverantwortliche
- **Umsetzungsverantwortliche:** IT-Betrieb, HR
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit

### 20.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

#### 20.5.1 Zugehörige Richtlinien

- 0230\_Richtlinie\_IAM\_Joiner\_Mover\_Leaver\_und\_Zugriffsantraege.md - Detaillierte IAM-Richtlinie
- 0240\_Policy\_Authentisierung\_und\_Passwoerter.md - Authentication Policy
- 0520\_Policy\_HR\_Security.md - HR Security Policy
- 0640\_Policy\_Ausnahmen\_und\_Risk\_Wavers.md - Exception Policy

#### 20.5.2 Zugehörige Standards/Baselins

- Rollenmodell und RBAC-Matrix
- Privileged Access Management (PAM) Standard
- Rezertifizierungsprozess
- Service-Account-Management

#### 20.5.3 Zugehörige Prozesse

- Joiner-Mover-Leaver-Prozess
- Zugriffsgenehmigungsprozess
- Rezertifizierungsprozess
- Incident Response bei unbefugtem Zugriff

## 20.6 6. Compliance, Monitoring und Durchsetzung

### 20.6.1 Messgrößen und KPIs

- Anzahl offener Zugriffsanträge und durchschnittliche Bearbeitungszeit
- Rezertifizierungsrate (Ziel: 100% jährlich)
- Anzahl nicht rezertifizierter Accounts
- Anzahl privilegierter Accounts und deren Nutzungshäufigkeit
- Anzahl Verstöße gegen Least Privilege
- Durchschnittliche Zeit zur Deaktivierung von Leaver-Accounts (Ziel: < 1 Tag)

### 20.6.2 Nachweise und Evidence

- IAM-System-Logs und Audit-Trails
- Zugriffsgenehmigungen und Anträge
- Rezertifizierungsnachweise
- Joiner-Mover-Leaver-Dokumentation
- Privileged Access Logs
- Audit-Berichte zu Zugriffsrechten

### 20.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:

- **Unbefugte Zugriffsvergabe:** Sofortige Sperrung, Untersuchung, ggf. Disziplinarmaßnahmen
- **Nicht rezertifizierte Accounts:** Automatische Deaktivierung nach Frist
- **Missbrauch privilegierter Zugriffe:** Sofortige Sperrung, arbeitsrechtliche Konsequenzen
- **Weitergabe von Zugangsdaten:** Verwarnung bis Kündigung

## 20.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und Ressourcen-Owner genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet und werden regelmäßig überprüft

## 20.8 8. Referenzen

### 20.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0230\_Richtlinie\_IAM\_Joiner\_Mover\_Leaver\_und\_Zugriffsantraege.md - Detailed IAM Guideline
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register
- 0530\_Richtlinie\_HR\_Onboarding\_Rollenwechsel\_Offboarding.md - HR Security Guideline

## 20.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.5.15 - Identity management
  - ISO/IEC 27001:2022 Annex A.5.16 - Access rights
  - ISO/IEC 27001:2022 Annex A.5.17 - Authentication information
  - ISO/IEC 27001:2022 Annex A.5.18 - Access rights review
  - ISO/IEC 27002:2022 - Information security controls
  - NIST SP 800-63 - Digital Identity Guidelines
- 

**Genehmigt durch:**

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 21

## Richtlinie: IAM - Joiner, Mover, Leaver und Zugriffsanträge

**Dokument-ID:** 0230

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0220\_Policy\_Zugriffssteuerung\_und\_Identitaetsmanagement.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.15, A.5.16, A.5.18

**Owner:** {{ meta.it\_operations.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 21.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0220\_Policy\_Zugriffssteuerung\_und\_Identitaetsmanagement.md und definiert detaillierte Prozesse für:  
- **Joiner:** Onboarding neuer Mitarbeiter und Zugriffsbereitstellung  
- **Mover:** Rollenwechsel und Zugriffsanpassungen  
- **Leaver:** Offboarding und Zugriffsentzug  
- **Zugriffsanträge:** Prozess für Ad-hoc-Zugriffsanforderungen

**Geltungsbereich:** Alle Mitarbeiter, Auftragnehmer und Dritte bei **AdminSend GmbH**

### 21.2 2. Joiner-Prozess (Onboarding)

#### 21.2.1 2.1 Prozessübersicht

**Trigger:** HR erstellt neuen Mitarbeiter in HR-System ({{ meta.hr.system }})

**Zeitrahmen:** - **Standard-Accounts:** Bereitstellung bis 1 Tag vor Arbeitsbeginn - **Spezial-Zugriffe:** Bereitstellung bis 3 Tage vor Arbeitsbeginn - **Externe Auftragnehmer:** Bereitstellung nach Vertragsunterzeichnung

## 21.2.2 2.2 Detaillierter Workflow

**Phase 1: HR-Initiierung (T-5 Tage)** 1. HR erstellt Mitarbeiterdatensatz in {{ meta.hr.system }} 2. HR definiert: - Abteilung, Rolle, Standort - Vorgesetzter, Kostenstelle - Startdatum, Vertragstyp (Festanstellung, Zeitarbeit, Praktikum) 3. Automatische Benachrichtigung an IT-Betrieb

**Phase 2: IT-Provisionierung (T-3 Tage)** 1. **Account-Erstellung:** - Active Directory / Azure AD Account - E-Mail-Postfach ({{ meta.email.system }}) - Benutzername nach Schema: {{ meta.naming.user\_format }} (z.B. vorname.nachname) - Initiales Passwort (temporär, muss bei erstem Login geändert werden)

### 2. Basis-Zugriffe (automatisch via Rollenmodell):

- Zugriff auf Intranet und Collaboration-Tools
- Standard-Anwendungen für Abteilung
- Netzlaufwerke gemäß Abteilungszugehörigkeit
- VPN-Zugang (falls Remote Work)

### 3. Hardware-Bereitstellung:

- Laptop/Desktop gemäß Rolle (siehe Hardware-Katalog)
- Mobilgerät (falls erforderlich)
- Peripherie (Monitor, Tastatur, Maus)
- Asset-Tagging und Inventarisierung

**Phase 3: Spezial-Zugriffe (T-2 Tage)** 1. Vorgesetzter beantragt spezielle Zugriffe über Self-Service-Portal 2. Genehmigung durch Ressourcen-Owner 3. Provisionierung durch IT-Betrieb oder automatisiert

**Phase 4: Onboarding-Tag (T-0)** 1. **Willkommens-E-Mail:** - Zugangsdaten (initiales Passwort) - Links zu Schulungen und Policies - Kontaktinformationen IT-Support 2. **Erste Anmeldung:** - Passwortänderung erzwungen - MFA-Registrierung (Authenticator-App, Hardware-Token) - Bestätigung der Acceptable Use Policy 3. **IT-Einweisung:** - Gerätenutzung, VPN-Zugang - Passwort-Manager-Schulung - Phishing-Awareness-Grundlagen

## 21.2.3 2.3 Rollenbasierte Zugriffe (RBAC)

### Standard-Rollen:

Rolle	Beschreibung	Automatische Zugriffe
Employee_Standard	All Mitarbeiter	Intranet, E-Mail, Office 365, VPN
Employee_Developer	Entwickler	+ Git, CI/CD, Dev-Umgebungen
Employee_Finance	Finanzabteilung	+ ERP, Buchhaltungssoftware
Employee_HR	Personalabteilung	+ HR-System, Bewerbermanagement
Employee_Sales	Vertrieb	+ CRM, Angebotssystem
Contractor_Standard	Externe Auftragnehmer	Basis-Zugriffe, zeitlich befristet
Contractor_Developer	Externe Entwickler	+ Dev-Zugriffe, zeitlich befristet

**Privilegierte Rollen:** - **Admin\_System:** Systemadministratoren (Windows, Linux) - **Admin\_Network:** Netzwerkadministratoren - **Admin\_Security:** Security-Team - **Admin\_Database:** Datenbankadministratoren

## 21.2.4 2.4 Externe Auftragnehmer und Dritte

**Besonderheiten:** - **Vertragsprüfung:** IT-Zugriff nur nach Vertragsunterzeichnung und NDA - **Zeitliche Befristung:** Accounts automatisch deaktiviert nach Vertragsende - **Eingeschränkte Zugriffe:** Nur projektbezogene Ressourcen - **Sponsorship:** Jeder externe Account benötigt internen Sponsor - **Rezertifizierung:** Quartalsweise Überprüfung durch Sponsor

## 21.3 3. Mover-Prozess (Rollenwechsel)

### 21.3.1 3.1 Prozessübersicht

**Trigger:** HR aktualisiert Mitarbeiterdaten (Abteilungswechsel, Beförderung, neue Rolle)

**Zeitrahmen:** Zugriffsanpassung innerhalb 2 Arbeitstagen nach HR-Änderung

### 21.3.2 3.2 Detaillierter Workflow

**Phase 1: HR-Änderung** 1. HR aktualisiert Mitarbeiterdatensatz in {{ meta.hr.system }} 2. Änderungen: Abteilung, Rolle, Vorgesetzter, Standort 3. Automatische Benachrichtigung an IT-Betrieb und bisherigen/neuen Vorgesetzten

**Phase 2: Zugriffs-Review** 1. **Alter Vorgesetzter:** Bestätigt Entzug nicht mehr benötigter Zugriffe 2. **Neuer Vorgesetzter:** Beantragt neue erforderliche Zugriffe 3. **IT-Betrieb:** Prüft aktuelle Zugriffe und plant Änderungen

**Phase 3: Zugriffsanpassung** 1. **Entzug alter Zugriffe:** - Entfernung aus alten Abteilungsgruppen - Entzug abteilungsspezifischer Anwendungszugriffe - Archivierung alter E-Mails (falls Postfachwechsel) 2. **Bereitstellung neuer Zugriffe:** - Hinzufügen zu neuen Abteilungs-Gruppen - Provisionierung neuer Anwendungszugriffe - Anpassung Netzlaufwerke und Berechtigungen

**Phase 4: Dokumentation** 1. Aktualisierung CMDB und Asset-Management 2. Dokumentation der Zugriffsänderungen 3. Benachrichtigung an Mitarbeiter über Änderungen

### 21.3.3 3.3 Beförderungen und Privilegien-Erhöhung

**Zusätzliche Prüfungen bei Privilegien-Erhöhung:** - **Genehmigung:** CISO-Genehmigung für privilegierte Rollen - **Background Check:** Erweiterte Überprüfung bei Admin-Rechten - **Schulung:** Zusätzliche Security-Schulungen für privilegierte Nutzer - **Monitoring:** Erhöhtes Monitoring privilegierter Aktivitäten

## 21.4 4. Leaver-Prozess (Offboarding)

### 21.4.1 4.1 Prozessübersicht

**Trigger:** HR markiert Mitarbeiter als ausscheidend in {{ meta.hr.system }}

**Zeitrahmen:** - **Geplantes Ausscheiden:** Deaktivierung am letzten Arbeitstag - **Ungeplantes Ausscheiden:** Sofortige Deaktivierung (z.B. Kündigung, Notfall)

## 21.4.2 4.2 Detaillierter Workflow

**Phase 1: Vorbereitung (T-14 Tage)** 1. HR informiert IT-Betrieb über Austrittsdatum 2. **Wissenstransfer:** - Vorgesetzter identifiziert kritische Zugriffe und Informationen - Übergabe an Nachfolger oder Team - Dokumentation von Passwörtern für Shared Accounts (in Password Manager) 3. **Daten-Backup:** - Sicherung persönlicher Laufwerke - Archivierung E-Mail-Postfach - Übergabe projektrelevanter Dateien

**Phase 2: Letzter Arbeitstag (T-0)** 1. **Account-Deaktivierung (End of Business Day):** - Active Directory / Azure AD Account deaktiviert - E-Mail-Weiterleitung an Vorgesetzten (temporär, 30 Tage) - VPN-Zugang gesperrt - Alle Anwendungszugriffe entzogen 2. **Hardware-Rückgabe:** - Laptop, Mobilgerät, Peripherie - Zutrittskarten, Schlüssel - Asset-Inventar aktualisiert 3. **Exit-Interview:** - Rückgabe aller Unternehmenseigentum - Erinnerung an Vertraulichkeitsverpflichtungen - Bestätigung der Datenrückgabe

**Phase 3: Post-Offboarding (T+30 Tage)** 1. **Account-Löschtung:** - Nach 30 Tagen: Endgültige Löschtung des Accounts - E-Mail-Archivierung gemäß Retention Policy ({{ meta.retention.email\_years }} Jahre) - Löschtung persönlicher Daten (DSGVO-konform) 2. **Lizenz-Freigabe:** - Rückgabe von Software-Lizenzen - Aktualisierung Lizenz-Management 3. **Dokumentation:** - Offboarding-Checkliste abgeschlossen - Audit-Trail für Compliance

## 21.4.3 4.3 Notfall-Offboarding

**Sofortige Deaktivierung bei:** - Kündigung aus wichtigem Grund - Sicherheitsvorfälle oder Verdacht auf Missbrauch - Gerichtliche Anordnungen

**Prozess:** 1. **Sofortige Sperrung (innerhalb 1 Stunde):** - Alle Accounts deaktiviert - VPN und Remote-Zugriffe gesperrt - Zutrittskarten deaktiviert - Mobilgeräte remote gelöscht (falls MDM) 2. **Forensik:** - Sicherung von Logs und Aktivitäten - Analyse bei Verdacht auf Datenmissbrauch - Einbeziehung Legal und HR 3. **Kommunikation:** - Information an Vorgesetzten und Security-Team - Dokumentation für rechtliche Zwecke

## 21.5 5. Zugriffsanträge (Access Requests)

### 21.5.1 5.1 Self-Service-Portal

**Zugriff:** {{ meta.iam.portal\_url }}

**Funktionen:** - Antrag auf neue Zugriffe (Anwendungen, Netzlaufwerke, Gruppen) - Übersicht eigener Zugriffe - Status-Tracking von Anträgen - Rezertifizierung eigener Zugriffe

### 21.5.2 5.2 Antrags-Workflow

**Schritt 1: Antragstellung** 1. Mitarbeiter stellt Antrag über Self-Service-Portal 2. **Pflichtangaben:** - Ressource/Anwendung - Begründung (Business Justification) - Benötigte Berechtigungsstufe - Zeitraum (permanent oder befristet)

**Schritt 2: Genehmigung** 1. **Vorgesetzter:** Prüft geschäftliche Notwendigkeit (1. Genehmigung) 2. **Ressourcen-Owner:** Prüft fachliche Berechtigung (2. Genehmigung) 3. **CISO:** Zusätzliche Genehmigung bei privilegierten Zugriffen 4. **Automatische Genehmigung:** Bei Standard-Zugriffen nach Rollenmodell

**Schritt 3: Provisionierung** 1. **Automatisch:** Bei Standard-Anwendungen (innerhalb 15 Minuten) 2. **Manuell:** Bei Spezial-Zugriffen (innerhalb 1 Arbeitstag) 3. **Benachrichtigung:** E-Mail an Antragsteller bei Abschluss

**Schritt 4: Dokumentation** 1. Audit-Trail im IAM-System 2. Aktualisierung CMDB 3. Compliance-Reporting

### 21.5.3 5.3 Befristete Zugriffe

**Anwendungsfälle:** - Projektbezogene Zugriffe - Vertretungen (Urlaub, Krankheit) - Externe Auftragnehmer - Test- und Entwicklungszugriffe

**Automatische Deaktivierung:** - System deaktiviert Zugriff automatisch nach Ablaufdatum - Benachrichtigung an Nutzer 7 Tage vor Ablauf - Verlängerung nur über erneuten Antrag

## 21.6 6. Rezertifizierung

### 21.6.1 6.1 Regelmäßige Zugriffs-Reviews

**Frequenz:** - **Standard-Nutzer:** Jährliche Rezertifizierung - **Privilegierte Nutzer:** Quartalsweise Rezertifizierung - **Externe Auftragnehmer:** Quartalsweise Rezertifizierung - **Kritische Systeme:** Monatliche Rezertifizierung

### 21.6.2 6.2 Rezertifizierungs-Prozess

**Schritt 1: Automatische Kampagne** 1. IAM-System startet Rezertifizierungs-Kampagne 2. E-Mail an Vorgesetzte mit Liste der Mitarbeiter-Zugriffe 3. Deadline: 14 Tage für Bestätigung

**Schritt 2: Review durch Vorgesetzte** 1. Vorgesetzter prüft jeden Zugriff: - **Bestätigen:** Zugriff weiterhin erforderlich - **Entziehen:** Zugriff nicht mehr benötigt - **Eskalieren:** Unsicherheit, Rückfrage an Ressourcen-Owner 2. Dokumentation der Entscheidung

**Schritt 3: Automatische Durchsetzung** 1. Bestätigte Zugriffe bleiben aktiv 2. Nicht bestätigte Zugriffe werden nach Deadline automatisch entzogen 3. Eskalierte Fälle werden an CISO weitergeleitet

**Schritt 4: Reporting** 1. Compliance-Report für Audit 2. Identifikation von Zugriffs-Anomalien 3. Optimierung Rollenmodell

### 21.6.3 6.3 Privilegierte Zugriffe

**Zusätzliche Kontrollen:** - **Vier-Augen-Prinzip:** Zwei Genehmigungen erforderlich - **Just-in-Time (JIT) Access:** Privilegien nur bei Bedarf, zeitlich befristet - **Privileged Access Management (PAM):** Verwaltung über PAM-System ({{ meta.security.pam\_solution }}) - **Session-Recording:** Aufzeichnung privilegierter Sessions für Audit

## 21.7 7. Technische Implementierung

### 21.7.1 7.1 IAM-Technologie-Stack

**Systeme:** - **Identity Provider:** {{ meta.iam.idp }} (z.B. Azure AD, Okta) - **HR-System:** {{ meta.hr.system }} (z.B. SAP SuccessFactors, Workday) - **IAM-Portal:** {{ meta.iam.portal }}

}} (z.B. SailPoint, Saviynt) - **PAM-System:** {{ meta.security.pam\_solution }} (z.B. CyberArk, BeyondTrust) - **CMDB:** {{ meta.itsm.cmdb }} (z.B. ServiceNow, Jira Service Management)

**Integration:** - HR-System → IAM-System (automatische Synchronisation) - IAM-System → Active Directory / Azure AD (Provisionierung) - IAM-System → Anwendungen (SCIM, SAML, API)

## 21.7.2 7.2 Automatisierung

**Automatisierte Prozesse:** - Account-Erstellung bei Joiner (innerhalb 1 Stunde nach HR-Eintrag)  
- Rollenbasierte Zugriffsvergabe (RBAC) - Account-Deaktivierung bei Leaver (am letzten Arbeitstag)  
- Befristete Zugriffe (automatische Deaktivierung) - Rezertifizierungs-Kampagnen (automatischer Start)

**Manuelle Prozesse:** - Spezial-Zugriffe außerhalb Rollenmodell - Privilegierte Zugriffe (nach Genehmigung) - Notfall-Offboarding (sofortige Sperrung)

## 21.8 8. Compliance und Audit

### 21.8.1 8.1 Messgrößen (KPIs)

Metrik	Zielwert	Messung
Joiner-Provisionierung	< 1 Tag	IAM-System
Leaver-Deaktivierung	100% am letzten Tag	IAM-System
Zugriffsanträge (Bearbeitungszeit)	< 1 Arbeitstag	IAM-System
Rezertifizierung (Completion Rate)	> 95%	IAM-System
Verwaiste Accounts	0	Quartalsweise Prüfung

### 21.8.2 8.2 Audit-Nachweise

**Dokumentation:** - Joiner/Mover/Leaver-Logs (Audit-Trail) - Zugriffsanträge und Genehmigungen - Rezertifizierungs-Berichte - Privilegierte Zugriffe und Genehmigungen - Notfall-Offboarding-Dokumentation

**Audit-Frequenz:** - Interne Audits: Quartalsweise - Externe Audits: Jährlich (ISO 27001) - Ad-hoc-Audits: Bei Sicherheitsvorfällen

## 21.9 9. Referenzen

### 21.9.1 Interne Dokumente

- 0220\_Policy\_Zugriffssteuerung\_und\_Identitätsmanagement.md - Übergeordnete Policy
- 0250\_Richtlinie\_MFA\_Passwordregeln\_und\_Session\_Management.md - Authentifizierung
- 0530\_Richtlinie\_HR\_Onboarding\_Rollenwechsel\_Offboarding.md - HR Security
- 0640\_Policy\_Ausnahmen\_und\_Risk\_Wavers.md - Exception Process

### 21.9.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.5.15 - Access control
- ISO/IEC 27001:2022 Annex A.5.16 - Identity management

- ISO/IEC 27001:2022 Annex A.5.18 - Access rights
  - NIST SP 800-63 - Digital Identity Guidelines
- 

**Genehmigt durch:**

Thomas Weber, CISO

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 22

## Policy: Authentisierung und Passwörter

**Dokument-ID:** 0240

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.17, A.5.18 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 22.1 1. Zweck

Diese Policy definiert die Grundsätze für Authentisierung und Passwortmanagement der **AdminSend GmbH**. Sie stellt sicher, dass die Identität von Nutzern sicher verifiziert wird und Authentisierungsinformationen angemessen geschützt werden.

### 22.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Systeme:** Alle IT-Systeme, Anwendungen, Datenbanken, Netzwerke, Cloud-Services
- **Personen:** Alle Mitarbeiter, Auftragnehmer, Lieferanten und Dritte mit Zugang zu IT-Ressourcen
- **Authentisierungsmethoden:** Passwörter, Multi-Faktor-Authentisierung (MFA), biometrische Verfahren, Token
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_) zulässig.

## **22.3 3. Grundsätze (Policy Statements)**

### **22.3.1 3.1 Starke Authentisierung**

Alle Zugriffe auf IT-Systeme und Anwendungen erfordern eine sichere Authentisierung. Die Stärke der Authentisierung richtet sich nach dem Schutzbedarf der Ressource und dem Risiko.

### **22.3.2 3.2 Multi-Faktor-Authentisierung (MFA)**

Für den Zugriff auf kritische Systeme, privilegierte Accounts und Remote-Zugriffe ist Multi-Faktor-Authentisierung (MFA) verpflichtend. MFA kombiniert mindestens zwei unabhängige Faktoren:

- Wissen (Passwort, PIN) - Besitz (Token, Smartphone, Smartcard) - Biometrie (Fingerabdruck, Gesichtserkennung)

### **22.3.3 3.3 Passwortanforderungen**

Passwörter müssen folgenden Mindestanforderungen entsprechen: - Ausreichende Länge und Komplexität (Details in Richtlinie) - Keine Wiederverwendung alter Passwörter - Keine Weitergabe oder Aufschreibung - Regelmäßige Änderung bei Verdacht auf Kompromittierung

### **22.3.4 3.4 Passwortlose Authentisierung**

Die Organisation fördert den Einsatz passwortloser Authentisierungsmethoden (z.B. FIDO2, Windows Hello, biometrische Verfahren) wo technisch möglich und sicher.

### **22.3.5 3.5 Session Management**

Authentisierte Sitzungen (Sessions) werden durch geeignete Maßnahmen geschützt: - Automatische Sperrung bei Inaktivität - Sichere Session-Token - Logout-Funktionalität - Keine parallelen Sessions für privilegierte Accounts

### **22.3.6 3.6 Schutz von Authentisierungsinformationen**

Passwörter und andere Authentisierungsinformationen werden sicher gespeichert: - Verschlüsselte oder gehashte Speicherung (keine Klartext-Passwörter) - Sichere Übertragung (TLS/SSL) - Schutz vor Brute-Force-Angriffen (Account-Lockout, Rate-Limiting)

### **22.3.7 3.7 Privilegierte Accounts**

Privilegierte Accounts (Administratoren, Root, Service-Accounts) unterliegen strengerer Authentisierungsanforderungen: - Verpflichtende MFA - Separate Accounts für privilegierte Tätigkeiten - Just-in-Time (JIT) Access wo möglich - Umfassende Protokollierung

### **22.3.8 3.8 Passwort-Reset und Account-Recovery**

Passwort-Reset- und Account-Recovery-Prozesse müssen sicher gestaltet sein und die Identität des Nutzers verifizieren, bevor Zugriff gewährt wird.

## 22.4 4. Rollen und Verantwortlichkeiten

### 22.4.1 RACI-Matrix: Authentisierung und Passwörter

Aktivität	CISO	IT-Betrieb	Mitarbeiter	IAM-Team	Security Operations
Policy-Erstellung	R/A	C	I	C	C
MFA-Implementierung	A	R	I	R	C
Passwort-Reset	I	R	R	R	I
Session-Monitoring	C	C	I	C	R/A
Brute-Force-Schutz	A	R	I	C	R
Incident Response	R/A	C	I	C	R

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

### 22.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **IAM-Verantwortlicher:** {{ meta.it.iam\_manager }}
- **Umsetzungsverantwortliche:** IT-Betrieb, IAM-Team
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit, Security Operations

## 22.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

### 22.5.1 Zugehörige Richtlinien

- **0250\_Richtlinie\_MFA\_Passwortregeln\_und\_Session\_Management.md** - Detaillierte Implementierungsrichtlinie
- **0220\_Policy\_Zugriffssteuerung\_und\_Identitätsmanagement.md** - Access Control Policy
- **0260\_Policy\_Kryptografie\_und\_Schlüsselmanagement.md** - Cryptography Policy
- **0400\_Policy\_Incident\_Management.md** - Incident Management Policy

### 22.5.2 Zugehörige Standards/Baselinses

- Passwort-Komplexitätsanforderungen
- MFA-Implementierungsstandard
- Session-Timeout-Konfigurationen
- Privileged Access Management (PAM) Standard

### 22.5.3 Zugehörige Prozesse

- Passwort-Reset-Prozess
- Account-Recovery-Prozess
- MFA-Enrollment-Prozess
- Incident Response bei Authentisierungsvorfällen

## 22.6 6. Compliance, Monitoring und Durchsetzung

### 22.6.1 Messgrößen und KPIs

- MFA-Adoption-Rate (Ziel: 100% für kritische Systeme)
- Anzahl Passwort-Reset-Anfragen pro Monat
- Anzahl fehlgeschlagener Authentisierungsversuche
- Anzahl Account-Lockouts
- Durchschnittliche Passwort-Stärke (Entropy)
- Anzahl kompromittierter Accounts

### 22.6.2 Nachweise und Evidence

- Authentisierungs-Logs und Audit-Trails
- MFA-Enrollment-Status
- Passwort-Policy-Compliance-Reports
- Brute-Force-Detection-Logs
- Incident-Reports bei Authentisierungsvorfällen
- Penetration-Test-Ergebnisse

### 22.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt: -

**Schwache Passwörter:** Erzwungene Passwortänderung, Nachschulung - **Passwort-Weitergabe:**

Verwarnung bis Kündigung - **MFA-Umgehung:** Sofortige Sperrung, Untersuchung - **Wiederholte**

**Verstöße:** Arbeitsrechtliche Konsequenzen

## 22.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet und werden regelmäßig überprüft
- **Kompensationsmaßnahmen:** Ausnahmen erfordern alternative Sicherheitsmaßnahmen

## 22.8 8. Referenzen

### 22.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy

- 0250\_Richtlinie\_MFA\_Passwortregeln\_und\_Session\_Management.md - Detailed Guideline
- 0220\_Policy\_Zugriffssteuerung\_und\_Identitätsmanagement.md - Access Control Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

## 22.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.5.17 - Authentication information
  - ISO/IEC 27001:2022 Annex A.5.18 - Access rights review
  - ISO/IEC 27002:2022 - Information security controls
  - NIST SP 800-63B - Digital Identity Guidelines: Authentication and Lifecycle Management
  - NIST SP 800-63-3 - Digital Identity Guidelines
  - BSI TR-02102 - Kryptographische Verfahren: Empfehlungen und Schlüssellängen
- 

### Genehmigt durch:

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

Nächster Review: {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 23

## Richtlinie: MFA, Passwortregeln und Session Management

**Dokument-ID:** 0250

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0240\_Policy\_Authentisierung\_und\_Passwoerter.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.17, A.5.18

**Owner:** {{ meta.it\_operations.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 23.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0240\_Policy\_Authentisierung\_und\_Passwoerter.md und definiert detaillierte Regeln für: - Multi-Faktor-Authentifizierung (MFA) - Passwortrichtlinien und Komplexitätsanforderungen - Session Management und Timeouts - Authentifizierungsmethoden und -technologien

**Geltungsbereich:** Alle Systeme, Anwendungen und Nutzer bei AdminSend GmbH

### 23.2 2. Multi-Faktor-Authentifizierung (MFA)

#### 23.2.1 2.1 MFA-Pflicht

**Obligatorisch für:** - Alle Remote-Zugriffe (VPN, Remote Desktop) - Alle privilegierten Accounts (Administratoren, Root) - Zugriff auf kritische Systeme (Produktion, Finanzsysteme) - Cloud-Services und SaaS-Anwendungen - E-Mail-Zugriff von externen Geräten - Zugriff auf vertrauliche Daten

- Optional für:** - Lokale Anmeldungen im Büro (kann durch Conditional Access erzwungen werden)  
 - Nicht-kritische interne Anwendungen

### 23.2.2 2.2 MFA-Methoden

#### Unterstützte Faktoren:

Methode	Typ	Sicherheitsstufe	Anwendungsfall
Authenticator-App (TOTP)	Besitz	Hoch	Standard für alle Nutzer
Hardware-Token (FIDO2/U2F)	Besitz	Sehr hoch	Privilegierte Nutzer, Hochsicherheit
SMS-Code	Besitz	Mittel	Fallback, nicht empfohlen
Push-Benachrichtigung	Besitz	Hoch	Mobile Nutzer
Biometrie (Fingerabdruck, Face ID)	Inhärenz	Hoch	Mobile Geräte, Windows Hello

**Empfohlene Methode:** Authenticator-App (z.B. Microsoft Authenticator, Google Authenticator, Authy)

**Nicht erlaubt:** - E-Mail-basierte Codes (zu unsicher) - Sicherheitsfragen (anfällig für Social Engineering)

### 23.2.3 2.3 MFA-Registrierung

**Onboarding:** 1. Neue Mitarbeiter registrieren MFA am ersten Arbeitstag 2. IT-Support unterstützt bei Einrichtung 3. Mindestens 2 MFA-Methoden registrieren (Primary + Backup) 4. Backup-Codes generieren und sicher aufbewahren

**Self-Service:** - Nutzer können MFA-Methoden über Self-Service-Portal verwalten - Änderung von MFA-Methoden erfordert Re-Authentifizierung - Verlust von MFA-Gerät: IT-Support-Prozess für Reset

### 23.2.4 2.4 MFA-Bypass und Notfallzugriff

**Break-Glass-Accounts:** - Notfall-Accounts ohne MFA für Systemwiederherstellung - Gesichert in Safe, nur für Notfälle - Nutzung wird sofort an CISO eskaliert - Passwort nach jeder Nutzung ändern

**Temporärer MFA-Bypass:** - Nur in Ausnahmefällen (z.B. Geräteverlust) - Genehmigung durch IT-Security erforderlich - Maximal 24 Stunden, dann automatische Sperrung - Erhöhtes Monitoring während Bypass-Zeitraum

## 23.3 3. Passwortrichtlinien

### 23.3.1 3.1 Passwortkomplexität

**Anforderungen für Standard-Nutzer:** - **Mindestlänge:** 12 Zeichen - **Komplexität:** Mindestens 3 von 4 Zeichentypen: - Großbuchstaben (A-Z) - Kleinbuchstaben (a-z) - Ziffern (0-9) - Sonderzeichen (!@#\$%^&\*) - **Keine Wörterbuch-Wörter:** Passwort darf nicht in Common-Password-Liste enthalten sein - **Keine persönlichen Informationen:** Kein Name, Geburtsdatum, Benutzername

**Anforderungen für privilegierte Nutzer:** - **Mindestlänge:** 16 Zeichen - **Komplexität:** Alle 4 Zeichentypen erforderlich - **Passphrase empfohlen:** Z.B. "Kaffee!Morgen@2024#Sicher"

**Technische Durchsetzung:** - Active Directory Group Policy Objects (GPOs) - Azure AD Password Protection - Passwort-Filter für Common-Password-Prüfung

### 23.3.2 3.2 Passwortänderung

**Regelmäßige Änderung:** - **Standard-Nutzer:** Alle 90 Tage (optional, wenn MFA aktiv) - **Privilegierte Nutzer:** Alle 60 Tage (verpflichtend) - **Service-Accounts:** Alle 180 Tage oder bei Personalwechsel

**Erzwungene Änderung:** - Bei erstem Login (initiales Passwort) - Nach Passwort-Reset durch IT-Support - Bei Verdacht auf Kompromittierung - Nach Sicherheitsvorfällen

**Passwort-Historie:** - Letzten 12 Passwörter dürfen nicht wiederverwendet werden - Verhindert Rotation zwischen wenigen Passwörtern

### 23.3.3 3.3 Passwort-Reset

**Self-Service Password Reset (SSPR):** - Nutzer können Passwort selbst zurücksetzen über {{meta.iam.sspr\_url}} - Verifizierung über: - MFA-Methode (Authenticator-App, SMS) - Alternative E-Mail-Adresse - Sicherheitsfragen (nur als Fallback) - Audit-Log für alle Passwort-Resets

**IT-Support-Reset:** - Bei Verlust aller SSPR-Methoden - Identitätsprüfung erforderlich (Personalausweis, Mitarbeiter-ID) - Temporäres Passwort, muss bei erstem Login geändert werden - Dokumentation im Ticketsystem

**Notfall-Reset:** - Bei gesperrten Accounts außerhalb Geschäftszeiten - On-Call IT-Support verfügbar - Erhöhte Verifizierung (Vorgesetzten-Bestätigung)

### 23.3.4 3.4 Passwort-Manager

**Empfehlung:** - Nutzung von Passwort-Manager für alle Nutzer - Unternehmens-Lösung: {{meta.security.password\_manager}} (z.B. 1Password, Bitwarden) - Zentrale Verwaltung von Shared Credentials

**Funktionen:** - Generierung starker, zufälliger Passwörter - Sichere Speicherung verschlüsselt - Browser-Integration für Auto-Fill - Sharing von Credentials im Team (verschlüsselt) - Audit-Log für Zugriffe

**Schulung:** - Onboarding-Schulung für neue Mitarbeiter - Best Practices für Passwort-Manager-Nutzung - Vermeidung von Passwort-Wiederverwendung

## 23.4 4. Session Management

### 23.4.1 4.1 Session-Timeouts

**Inaktivitäts-Timeouts:**

System-Typ	Timeout	Begründung
Workstation (lokal)	15 Minuten	Physischer Zugriff möglich
VPN-Verbindung	8 Stunden	Remote-Zugriff, Re-Auth täglich
Web-Anwendungen	30 Minuten	Balance zwischen Sicherheit und Usability
Privilegierte Sessions	10 Minuten	Erhöhtes Risiko
Mobile Apps	5 Minuten	Geräteverlust-Risiko

**Absolute Session-Limits:** - **Standard-Nutzer:** Max. 12 Stunden, dann Re-Authentifizierung - **Privilegierte Nutzer:** Max. 4 Stunden, dann Re-Authentifizierung - **Remote-Zugriffe:** Max. 8 Stunden, dann Re-Authentifizierung

### 23.4.2 4.2 Bildschirmsperre

**Automatische Sperre:** - Nach Inaktivitäts-Timeout (siehe oben) - Entsperren nur mit Passwort oder Biometrie - Keine Anzeige sensibler Informationen auf Sperrbildschirm

**Manuelle Sperre:** - Nutzer müssen Workstation sperren beim Verlassen (Windows+L, Ctrl+Alt+Del) - Awareness-Kampagnen zu "Clean Desk Policy" - Stichproben durch Security-Team

### 23.4.3 4.3 Concurrent Sessions

**Limits:** - **Standard-Nutzer:** Max. 3 gleichzeitige Sessions - **Privilegierte Nutzer:** Max. 2 gleichzeitige Sessions - **Service-Accounts:** Max. 1 Session (verhindert Credential-Sharing)

**Monitoring:** - Alerts bei ungewöhnlichen Session-Mustern - Automatische Sperrung bei Verdacht auf Account-Sharing - Geolocation-Checks (unmögliche Reisen)

### 23.4.4 4.4 Session-Sicherheit

**Technische Kontrollen:** - **Session-Tokens:** Kryptographisch sichere, zufällige Tokens - **Token-Rotation:** Neue Tokens nach Re-Authentifizierung - **Secure Cookies:** HttpOnly, Secure, Same-Site Flags - **Session-Fixation-Schutz:** Neue Session-ID nach Login - **HTTPS-Erzwingung:** Alle Sessions über verschlüsselte Verbindungen

## 23.5 5. Authentifizierungsmethoden

### 23.5.1 5.1 Single Sign-On (SSO)

**Implementierung:** - **Identity Provider:** {{ meta.iam.idp }} (z.B. Azure AD, Okta) - **Protokolle:** SAML 2.0, OAuth 2.0, OpenID Connect - **Anwendungen:** Alle Cloud-SaaS-Anwendungen über SSO

**Vorteile:** - Einmalige Anmeldung für alle Anwendungen - Zentrale Authentifizierung und MFA - Reduzierte Passwort-Müdigkeit - Vereinfachtes Offboarding (zentrale Sperrung)

**Conditional Access:** - Risikobasierte Authentifizierung - Geräte-Compliance-Checks - Geolocation-basierte Policies - Erzwingung von MFA bei erhöhtem Risiko

### 23.5.2 5.2 Zertifikat-basierte Authentifizierung

**Anwendungsfälle:** - Maschine-zu-Maschine-Authentifizierung - VPN-Zugriff (zusätzlich zu MFA) - Wireless-Netzwerk (802.1X) - Code-Signing und E-Mail-Verschlüsselung

**PKI-Infrastruktur:** - Interne Certificate Authority (CA): {{ meta.pki.ca }} - Zertifikats-Lebenszyklus-Management - Automatische Erneuerung vor Ablauf - Revocation-Checks (CRL, OCSP)

### 23.5.3 5.3 Biometrische Authentifizierung

**Unterstützte Methoden:** - Windows Hello for Business: Fingerabdruck, Gesichtserkennung - **Mobile Geräte:** Touch ID, Face ID - **Nur als zweiter Faktor:** Biometrie ersetzt nicht Passwort

**Datenschutz:** - Biometrische Daten werden lokal auf Gerät gespeichert (nicht zentral) - Keine Übertragung biometrischer Rohdaten - DSGVO-konforme Verarbeitung

## 23.6 6. Service-Accounts und technische Accounts

### 23.6.1 6.1 Service-Account-Richtlinien

**Anforderungen:** - **Keine interaktiven Logins:** Service-Accounts dürfen nicht für menschliche Anmeldungen genutzt werden - **Starke Passwörter:** Mindestens 24 Zeichen, zufällig generiert - **Passwort-Rotation:** Alle 180 Tage oder bei Personalwechsel - **Dokumentation:** Zweck, Owner, verwendete Systeme

**Verwaltung:** - Zentrale Verwaltung in Passwort-Manager oder PAM-System - Genehmigung durch CISO für neue Service-Accounts - Regelmäßige Reviews (quartalsweise) - Deaktivierung ungenutzter Accounts

### 23.6.2 6.2 API-Keys und Tokens

**Best Practices:** - **Rotation:** API-Keys alle 90 Tage rotieren - **Least Privilege:** Minimale Berechtigungen für API-Keys - **Secrets Management:** Speicherung in Secrets-Manager (z.B. HashiCorp Vault, Azure Key Vault) - **Keine Hardcoding:** API-Keys nicht in Code oder Config-Dateien

**Monitoring:** - Logging aller API-Zugriffe - Alerts bei ungewöhnlichen API-Nutzungsmustern - Rate-Limiting für API-Calls

## 23.7 7. Monitoring und Alerting

### 23.7.1 7.1 Authentifizierungs-Monitoring

**Überwachte Events:** - Fehlgeschlagene Login-Versuche (Brute-Force-Detection) - Erfolgreiche Logins von ungewöhnlichen Standorten - MFA-Bypass-Versuche - Passwort-Resets (insbesondere privilegierte Accounts) - Concurrent Sessions von verschiedenen IPs

**Automatische Alerts:** - **5 fehlgeschlagene Logins:** Warnung an Nutzer - **10 fehlgeschlagene Logins:** Account-Sperrung (30 Minuten) - **Login von neuem Gerät/Standort:** MFA-Challenge - **Unmögliche Reise:** Alert an Security-Team (z.B. Login in Deutschland, 1 Stunde später in USA)

### 23.7.2 7.2 Account-Sperrung

**Automatische Sperrung:** - Nach 10 fehlgeschlagenen Login-Versuchen - Sperrdauer: 30 Minuten (automatische Entsperrung) - Manuelle Entsperrung durch IT-Support möglich

**Privilegierte Accounts:** - Bereits nach 5 fehlgeschlagenen Versuchen - Manuelle Entsperrung nur durch CISO oder IT-Security - Untersuchung bei Sperrung (möglicher Angriff)

## 23.8 8. Compliance und Audit

### 23.8.1 8.1 Messgrößen (KPIs)

Metrik	Zielwert	Messung
MFA-Adoption-Rate	> 99%	IAM-System
Passwort-Komplexität-Compliance	100%	AD-Reports
Fehlgeschlagene Logins	< 100 pro Tag	SIEM
Passwort-Resets	< 50 pro Monat	IAM-System
Session-Timeout-Compliance	> 95%	Endpoint-Monitoring

### 23.8.2 8.2 Audit-Nachweise

**Dokumentation:** - Authentifizierungs-Logs (Erfolg und Fehler) - MFA-Registrierungen und - Nutzung - Passwort-Änderungen und -Resets - Account-Sperrungen und Entsperrungen - Privilegierte Zugriffe

**Retention:** - Authentifizierungs-Logs: {{ meta.retention.log\_years }} Jahre - Audit-Trails: {{ meta.retention.audit\_years }} Jahre

## 23.9 9. Referenzen

### 23.9.1 Interne Dokumente

- 0240\_Policy\_Authentisierung\_und\_Passwoerter.md - Übergeordnete Policy
- 0230\_Richtlinie\_IAM\_Joiner\_Mover\_Leaver\_und\_Zugriffsantraege.md - IAM Processes
- 0320\_PolicyLogging\_und\_Monitoring.md - Logging Policy

### 23.9.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.5.17 - Authentication information
- ISO/IEC 27001:2022 Annex A.5.18 - Access rights
- NIST SP 800-63B - Digital Identity Guidelines (Authentication)
- OWASP Authentication Cheat Sheet

**Genehmigt durch:**

Thomas Weber, CISO

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 24

## Policy: Kryptografie und Schlüsselmanagement

**Dokument-ID:** 0260

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.8.24 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 24.1 1. Zweck

Diese Policy definiert die Grundsätze für den Einsatz kryptografischer Verfahren und das Management kryptografischer Schlüssel der **AdminSend GmbH**. Sie stellt sicher, dass Informationen durch angemessene kryptografische Kontrollen geschützt werden und Schlüssel sicher verwaltet werden.

### 24.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Systeme:** Alle IT-Systeme, Anwendungen, Datenbanken, Netzwerke, Cloud-Services
- **Daten:** Alle Daten in Ruhe (Data at Rest), in Bewegung (Data in Transit) und in Verarbeitung (Data in Use)
- **Kryptografische Verfahren:** Verschlüsselung, Hashing, digitale Signaturen, Zertifikate
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_) zulässig.

## **24.3 3. Grundsätze (Policy Statements)**

### **24.3.1 3.1 Risikoorientierter Einsatz von Kryptografie**

Kryptografische Verfahren werden auf Basis einer Risikoanalyse eingesetzt. Der Schutzbedarf der Informationen bestimmt die Stärke und Art der kryptografischen Kontrollen.

### **24.3.2 3.2 Verschlüsselung sensibler Daten**

Sensible und vertrauliche Daten werden sowohl bei der Speicherung (Data at Rest) als auch bei der Übertragung (Data in Transit) verschlüsselt: - **Data at Rest:** Verschlüsselung von Datenbanken, Dateisystemen, Backups, mobilen Geräten - **Data in Transit:** TLS/SSL für Netzwerkkommunikation, VPN für Remote-Zugriffe - **Data in Use:** Verschlüsselung im Arbeitsspeicher wo technisch möglich (z.B. Confidential Computing)

### **24.3.3 3.3 Verwendung anerkannter Algorithmen**

Es werden ausschließlich anerkannte und standardisierte kryptografische Algorithmen eingesetzt: - Symmetrische Verschlüsselung: AES-256 oder höher - Asymmetrische Verschlüsselung: RSA-2048 oder höher, ECC mit mindestens 256 Bit - Hashing: SHA-256 oder höher - Veraltete Algorithmen (MD5, SHA-1, DES, 3DES) sind untersagt

### **24.3.4 3.4 Schlüsselmanagement-Lebenszyklus**

Kryptografische Schlüssel werden über ihren gesamten Lebenszyklus sicher verwaltet: - **Generierung:** Sichere Zufallszahlengeneratoren, ausreichende Schlüssellänge - **Speicherung:** Hardware Security Modules (HSM), Key Management Systems (KMS) - **Verteilung:** Sichere Übertragungskanäle, Authentifizierung der Empfänger - **Rotation:** Regelmäßige Schlüsselrotation basierend auf Risiko und Compliance-Anforderungen - **Archivierung:** Sichere Aufbewahrung für Entschlüsselung historischer Daten - **Vernichtung:** Sichere Löschung nicht mehr benötigter Schlüssel

### **24.3.5 3.5 Trennung von Schlüsseln und Daten**

Kryptografische Schlüssel werden getrennt von den verschlüsselten Daten gespeichert. Schlüssel dürfen nicht im Klartext in Konfigurationsdateien oder Quellcode abgelegt werden.

### **24.3.6 3.6 Zertifikatsmanagement**

Digitale Zertifikate werden zentral verwaltet: - Verwendung vertrauenswürdiger Certificate Authorities (CA) - Regelmäßige Überprüfung und Erneuerung von Zertifikaten - Überwachung ablaufender Zertifikate - Sichere Speicherung privater Schlüssel

### **24.3.7 3.7 Kryptografische Protokolle**

Sichere kryptografische Protokolle werden für die Kommunikation verwendet: - TLS 1.2 oder höher (TLS 1.3 bevorzugt) - SSH-2 für sichere Remote-Zugriffe - IPsec für VPN-Verbindungen - Veraltete Protokolle (SSL, TLS 1.0/1.1) sind untersagt

### 24.3.8 3.8 Compliance mit Export-Kontrollen

Der Einsatz von Kryptografie erfolgt in Übereinstimmung mit nationalen und internationalen Export-Kontrollvorschriften.

## 24.4 4. Rollen und Verantwortlichkeiten

### 24.4.1 RACI-Matrix: Kryptografie und Schlüsselmanagement

Aktivität	CISO	IT-Betrieb	Crypto Officer	Entwicklung	Compliance
Policy-Erstellung	R/A	C	C	C	C
Krypto-Architektur	A	C	R	C	I
Schlüssel-Generierung	C	R	R/A	I	I
Schlüssel-Rotation	C	R	R/A	I	I
Zertifikats-Management	C	R	R/A	I	I
Krypto-Monitoring	A	C	R	I	C
Compliance-Prüfung	C	I	C	I	R/A

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

### 24.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **Crypto Officer:** {{ meta.it.crypto\_officer }}
- **Key Management Verantwortlicher:** {{ meta.it.key\_manager }}
- **Umsetzungsverantwortliche:** IT-Betrieb, Entwicklung
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit, Compliance

## 24.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

### 24.5.1 Zugehörige Richtlinien

- **0270\_Richtlinie\_Key\_Management\_und\_Verschluesselung.md** - Detaillierte Implementierungsrichtlinie
- **0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md** - Data Classification Policy
- **0460\_Policy\_Lieferanten\_und\_Cloud\_Sicherheit.md** - Cloud Security Policy

- 0600\_Policy\_Netzwerksicherheit.md - Network Security Policy

#### 24.5.2 Zugehörige Standards/Baselins

- Kryptografische Algorithmen-Standard
- Schlüssellängen-Anforderungen
- TLS/SSL-Konfigurationsstandard
- Zertifikats-Lifecycle-Standard

#### 24.5.3 Zugehörige Prozesse

- Schlüssel-Generierungs- und Rotationsprozess
- Zertifikats-Erneuerungsprozess
- Incident Response bei Schlüsselkompromittierung
- Krypto-Agility-Prozess (Migration zu neuen Algorithmen)

### 24.6 6. Compliance, Monitoring und Durchsetzung

#### 24.6.1 Messgrößen und KPIs

- Anzahl verschlüsselter Systeme und Datenbanken
- Verschlüsselungsrate sensibler Daten (Ziel: 100%)
- Anzahl ablaufender Zertifikate (Ziel: 0 abgelaufene Zertifikate)
- Durchschnittliche Schlüsselrotationszeit
- Anzahl Verstöße gegen Krypto-Standards
- Anzahl kompromittierter Schlüssel

#### 24.6.2 Nachweise und Evidence

- Verschlüsselungs-Inventar
- Schlüssel-Management-Logs
- Zertifikats-Register
- Krypto-Compliance-Reports
- Penetration-Test-Ergebnisse
- Audit-Berichte zu kryptografischen Kontrollen

#### 24.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:

- **Verwendung schwacher Algorithmen:** Sofortige Remediation, Nachschulung
- **Unsichere Schlüsselspeicherung:** Sofortige Schlüsselrotation, Untersuchung
- **Schlüsselkompromittierung:** Incident Response, Revocation, forensische Analyse
- **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen

### 24.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md

- **Genehmigung:** Ausnahmen müssen vom CISO und Crypto Officer genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet und werden regelmäßig überprüft
- **Kompensationsmaßnahmen:** Ausnahmen erfordern alternative Sicherheitsmaßnahmen

## 24.8 8. Referenzen

### 24.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0270\_Richtlinie\_Key\_Management\_und\_Verschluesselung.md - Detailed Guideline
- 0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md - Data Classification Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

### 24.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.8.24 - Use of cryptography
- ISO/IEC 27002:2022 - Information security controls
- NIST SP 800-57 - Recommendation for Key Management
- NIST SP 800-175B - Guideline for Using Cryptographic Standards
- BSI TR-02102 - Kryptographische Verfahren: Empfehlungen und Schlüssellängen
- FIPS 140-2/140-3 - Security Requirements for Cryptographic Modules
- eIDAS-Verordnung (EU 910/2014) - Elektronische Identifizierung und Vertrauensdienste

**Genehmigt durch:**

{{{ meta.management.ceo }}}, Geschäftsführung  
Datum: {{{ meta.document.approval\_date }}}

**Nächster Review:** {{{ meta.document.next\_review }}} (jährlich oder anlassbezogen)

ewpage

# Chapter 25

## Richtlinie: Key Management und Verschlüsselung

**Dokument-ID:** 0270

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0260\_Policy\_Kryptografie\_und\_Schluesselmanagement.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.8.24

**Owner:** {{ meta.it\_operations.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Vertraulich

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 25.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0260\_Policy\_Kryptografie\_und\_Schluesselmanagement.md und definiert detaillierte Verfahren für:  
- Kryptographische Algorithmen und Standards  
- Schlüsselerzeugung, -speicherung und -rotation  
- Zertifikatsmanagement  
- Verschlüsselung von Daten in Ruhe und in Bewegung

**Geltungsbereich:** Alle kryptographischen Systeme bei AdminSend GmbH

### 25.2 2. Kryptographische Standards

#### 25.2.1 2.1 Genehmigte Algorithmen

**Symmetrische Verschlüsselung:** - **AES-256** (Advanced Encryption Standard, 256-bit) - Empfohlen  
- **AES-128** - Akzeptabel für nicht-kritische Daten  
- **ChaCha20** - Akzeptabel für mobile Geräte

**Asymmetrische Verschlüsselung:** - **RSA-4096** - Empfohlen für langfristige Sicherheit  
- **RSA-2048** - Akzeptabel, Mindestanforderung  
- **ECDSA P-384** - Empfohlen für Performance  
- **Ed25519**

- Akzeptabel für SSH-Keys

**Hash-Funktionen:** - **SHA-256** - Mindestanforderung - **SHA-384, SHA-512** - Empfohlen für kritische Anwendungen - **BLAKE2** - Akzeptabel

**Verbotene Algorithmen:** - MD5, SHA-1 (kryptographisch gebrochen) - DES, 3DES (veraltet) - RSA < 2048 bit (zu schwach) - RC4 (unsicher)

## 25.2.2 2.2 TLS/SSL-Konfiguration

**TLS-Versionen:** - **TLS 1.3** - Empfohlen - **TLS 1.2** - Mindestanforderung - **TLS 1.1, 1.0, SSL** - Verboten

**Cipher Suites (Empfohlen):**

TLS\_AES\_256\_GCM\_SHA384

TLS\_CHACHA20\_POLY1305\_SHA256

TLS\_AES\_128\_GCM\_SHA256

ECDHE-RSA-AES256-GCM-SHA384

ECDHE-RSA-AES128-GCM-SHA256

**Zertifikate:** - Mindestens RSA-2048 oder ECDSA P-256 - Gültigkeitsdauer: Max. 13 Monate (398 Tage) - Trusted Certificate Authorities (CAs)

## 25.3 3. Schlüsselmanagement

### 25.3.1 3.1 Schlüsselerzeugung

**Anforderungen:** - Kryptographisch sichere Zufallszahlengeneratoren (CSPRNG) - Schlüssellängen gemäß Abschnitt 2.1 - Erzeugung in sicherer Umgebung (HSM, Key Vault)

**Prozess:** 1. Schlüsselanforderung über Ticketsystem 2. Genehmigung durch CISO oder IT-Security 3. Erzeugung durch Key Management System 4. Sichere Übergabe an Antragsteller 5. Dokumentation in Key-Register

### 25.3.2 3.2 Schlüsselspeicherung

**Hardware Security Modules (HSM):** - Kritische Schlüssel (Root-CA, Master-Keys) in HSM: {{ meta.security.hsm }} - FIPS 140-2 Level 2 oder höher - Physische Sicherheit und Zugriffskontrolle

**Key Management Systems:** - **Cloud:** {{ meta.cloud.key\_vault }} (z.B. Azure Key Vault, AWS KMS) - **On-Premises:** {{ meta.security.kms }} (z.B. HashiCorp Vault) - Verschlüsselte Speicherung - Audit-Logging aller Zugriffe

**Verboten:** - Speicherung in Klartext - Hardcoding in Quellcode - Speicherung in Konfigurationsdateien - Übertragung per E-Mail oder Chat

### 25.3.3 3.3 Schlüsselrotation

**Rotations-Intervalle:**

Schlüsseltyp	Rotation	Begründung
Daten-Verschlüsselungsschlüssel (DEK)	Jährlich	Balance zwischen Sicherheit und Aufwand
Key-Encryption-Keys (KEK)	Alle 2 Jahre	Selten genutzt, höhere Sicherheit
TLS-Zertifikate	Alle 12 Monate	CA-Anforderungen
API-Keys	Alle 90 Tage	Häufige Nutzung, höheres Risiko
SSH-Keys	Alle 180 Tage	Administrativer Zugriff

**Automatisierung:** - Automatische Rotation wo möglich (Cloud-Services) - Benachrichtigungen 30 Tage vor Ablauf - Dokumentation aller Rotationen

**Notfall-Rotation:** - Bei Verdacht auf Kompromittierung: Sofortige Rotation - Bei Personalwechsel: Rotation aller betroffenen Schlüssel - Bei Sicherheitsvorfällen: Rotation gemäß Incident Response

### 25.3.4 3.4 Schlüsselvernichtung

**Prozess:** 1. Schlüssel als “deprecated” markieren 2. Grace Period (30 Tage) für Datenentschlüsselung 3. Sichere Löschung aus allen Systemen 4. Dokumentation der Vernichtung

**Methoden:** - Kryptographisches Überschreiben (mehrfach) - HSM: Secure Erase-Funktion - Physische Medien: Zerstörung gemäß DIN 66399

## 25.4 4. Zertifikatsmanagement

### 25.4.1 4.1 Public Key Infrastructure (PKI)

**Komponenten:** - **Root CA:** {{ meta.pki.root\_ca }} (Offline, HSM-geschützt) - **Issuing CA:** {{ meta.pki.issuing\_ca }} (Online, für Zertifikatsausstellung) - **Certificate Management System:** {{ meta.pki.cms }}

**Zertifikatstypen:** - **Server-Zertifikate:** Web-Server, API-Endpoints - **Client-Zertifikate:** Benutzer-Authentifizierung, VPN - **Code-Signing:** Software-Signierung - **E-Mail-Zertifikate:** S/MIME-Verschlüsselung

### 25.4.2 4.2 Zertifikats-Lebenszyklus

**Ausstellung:** 1. Certificate Signing Request (CSR) erstellen 2. Antrag über PKI-Portal einreichen 3. Validierung durch Certificate Authority 4. Zertifikat ausstellen und bereitstellen 5. Installation und Konfiguration

**Erneuerung:** - Automatische Benachrichtigung 60 Tage vor Ablauf - Erneuerung 30 Tage vor Ablauf - Automatisierung über ACME-Protokoll (Let's Encrypt)

**Widerruf (Revocation):** - Bei Kompromittierung: Sofortiger Widerruf - Bei Personalwechsel: Widerruf aller persönlichen Zertifikate - Veröffentlichung in Certificate Revocation List (CRL) - OCSP (Online Certificate Status Protocol) für Echtzeit-Checks

### 25.4.3 4.3 Zertifikats-Inventar

**Dokumentation:** - Alle ausgestellten Zertifikate in CMDB - Ablaufdaten, Verwendungszweck, Owner - Automatische Scans für unbekannte Zertifikate

**Monitoring:** - Tägliche Prüfung auf ablaufende Zertifikate - Alerts bei Zertifikaten < 30 Tage Gültigkeit - Automatische Erneuerung wo möglich

## 25.5 5. Verschlüsselung von Daten

### 25.5.1 5.1 Data at Rest (Daten in Ruhe)

**Verschlüsselungspflicht:** - Alle vertraulichen und streng vertraulichen Daten - Personenbezogene Daten (DSGVO-Anforderung) - Finanzdaten und Geschäftsgeheimnisse - Backups und Archivdaten

**Methoden:**

Speicherort	Methode	Schlüsselverwaltung
Laptops/Desktops	BitLocker (Windows), FileVault (macOS)	TPM + Recovery Key in Key Vault
Server-Festplatten	LUKS (Linux), BitLocker (Windows)	Key Vault
Datenbanken	Transparent Data Encryption (TDE)	Database Key Management
Cloud-Storage	Server-Side Encryption (SSE)	Cloud Key Management Service
Dateiserver	Encrypted File System (EFS)	Active Directory + Key Vault

**Konfiguration:** - AES-256 für alle Verschlüsselungen - Automatische Verschlüsselung bei Speicherung - Keine Nutzer-Interaktion erforderlich

### 25.5.2 5.2 Data in Transit (Daten in Bewegung)

**Verschlüsselungspflicht:** - Alle Datenübertragungen über öffentliche Netzwerke - Interne Übertragungen vertraulicher Daten - API-Kommunikation - E-Mail mit vertraulichen Inhalten

**Methoden:**

Übertragungsart	Protokoll	Konfiguration
Web-Traffic	HTTPS (TLS 1.2+)	Siehe Abschnitt 2.2
E-Mail	TLS (SMTP), S/MIME	Opportunistic TLS + Verschlüsselung für vertraulich
Dateittransfer	SFTP, FTPS, HTTPS	Keine unverschlüsselten Protokolle
VPN	IPsec, WireGuard	AES-256, Perfect Forward Secrecy

Übertragungsart	Protokoll	Konfiguration
Database	TLS für Verbindungen	Erzwungene Verschlüsselung

**Verbotene Protokolle:** - FTP (unverschlüsselt) - Telnet (unverschlüsselt) - HTTP für vertrauliche Daten - SMTP ohne TLS für vertrauliche E-Mails

### 25.5.3 5.3 Data in Use (Daten in Verarbeitung)

**Technologien:** - **Confidential Computing:** Verschlüsselung während Verarbeitung (Intel SGX, AMD SEV) - **Homomorphic Encryption:** Berechnungen auf verschlüsselten Daten (experimentell) - **Secure Enclaves:** Isolierte Verarbeitungsumgebungen

**Anwendungsfälle:** - Verarbeitung hochsensibler Daten in Cloud - Multi-Party-Computation - Privacy-Preserving Analytics

## 25.6 6. E-Mail-Verschlüsselung

### 25.6.1 6.1 S/MIME

**Implementierung:** - S/MIME-Zertifikate für alle Mitarbeiter - Automatische Verschlüsselung für E-Mails mit "Vertraulich"-Klassifizierung - Signierung aller ausgehenden E-Mails

**Konfiguration:** - Outlook, Thunderbird: S/MIME-Plugin - Mobile Geräte: Native S/MIME-Unterstützung - Zertifikatsverteilung über Active Directory

### 25.6.2 6.2 Opportunistic TLS

**SMTP TLS:** - Alle E-Mail-Server unterstützen STARTTLS - Erzwungene Verschlüsselung für bekannte Partner - Fallback auf unverschlüsselt nur für nicht-vertrauliche E-Mails

**MTA-STS (Mail Transfer Agent Strict Transport Security):** - Policy-Veröffentlichung über DNS - Erzwingung von TLS für eingehende E-Mails

## 25.7 7. Backup-Verschlüsselung

**Anforderungen:** - Alle Backups verschlüsselt (AES-256) - Separate Schlüssel für Backups (nicht Produktionsschlüssel) - Offline-Kopie der Backup-Schlüssel (Safe)

**Prozess:** 1. Backup-Erstellung mit Verschlüsselung 2. Schlüssel in Key Vault speichern 3. Offline-Kopie des Schlüssels in Safe 4. Regelmäßige Restore-Tests (quartalsweise)

**Disaster Recovery:** - Backup-Schlüssel in Notfall-Dokumentation - Zugriff nur durch autorisierte Personen - Vier-Augen-Prinzip für Schlüsselzugriff

## 25.8 8. Cloud-Verschlüsselung

### 25.8.1 8.1 Cloud Storage

**Konfiguration:** - **Azure:** Customer-Managed Keys (CMK) in Azure Key Vault - **AWS:** Customer Master Keys (CMK) in AWS KMS - **Google Cloud:** Customer-Managed Encryption Keys

(CMEK)

**Vorteile:** - Kontrolle über Schlüssel - Möglichkeit zur Schlüsselrotation - Compliance-Anforderungen erfüllt

## 25.8.2 8.2 Cloud Databases

**Verschlüsselung:** - Transparent Data Encryption (TDE) aktiviert - Verschlüsselte Verbindungen (TLS) - Customer-Managed Keys für kritische Datenbanken

# 25.9 9. Compliance und Audit

## 25.9.1 9.1 Messgrößen (KPIs)

Metrik	Zielwert	Messung
Verschlüsselte Laptops	100%	Endpoint-Management
TLS 1.2+ Nutzung	100%	Web-Server-Logs
Zertifikats-Ablauf-Incidents	0 pro Jahr	PKI-Monitoring
Schlüsselrotation-Compliance	> 95%	Key Management System

## 25.9.2 9.2 Audit-Nachweise

**Dokumentation:** - Kryptographie-Policy und -Richtlinien - Schlüssel-Register und -Inventar - Zertifikats-Inventar - Verschlüsselungs-Konfigurationen - Audit-Logs für Schlüsselzugriffe

# 25.10 10. Referenzen

## 25.10.1 Interne Dokumente

- 0260\_Policy\_Kryptografie\_und\_Schluesselmanagement.md - Übergeordnete Policy
- 0420\_Policy\_Backup\_und\_Wiederherstellung.md - Backup Policy

## 25.10.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.8.24 - Use of cryptography
- NIST SP 800-57 - Key Management Recommendations
- NIST SP 800-52 - TLS Guidelines
- BSI TR-02102 - Kryptographische Verfahren

---

### Genehmigt durch:

Thomas Weber, CISO

Datum: {{ meta.document.approval\_date }}

Nächster Review: {{ meta.document.next\_review }}

ewpage

# Chapter 26

## Policy: Datenklassifizierung und Informationshandling

**Dokument-ID:** 0280

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.12-A.5.14 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 26.1 1. Zweck

Diese Policy definiert die Grundsätze für Datenklassifizierung und Informationshandling der **AdminSend GmbH**. Sie stellt sicher, dass Informationen entsprechend ihrer Sensitivität und ihres Schutzbedarfs klassifiziert, gekennzeichnet und über ihren gesamten Lebenszyklus angemessen geschützt werden.

### 26.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Informationen:** Alle Informationen in jeglicher Form (digital, physisch, mündlich)
- **Systeme:** Alle IT-Systeme, Anwendungen, Datenbanken, Speichermedien
- **Personen:** Alle Mitarbeiter, Auftragnehmer, Lieferanten und Dritte mit Zugang zu Informationen
- **Lebenszyklus:** Erstellung, Speicherung, Verarbeitung, Übertragung, Archivierung, Vernichtung
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_) zulässig.

## 26.3 3. Grundsätze (Policy Statements)

### 26.3.1 3.1 Verpflichtende Klassifizierung

Alle Informationen der Organisation müssen klassifiziert werden. Die Klassifizierung erfolgt durch den Information Owner basierend auf Vertraulichkeit, Integrität und Verfügbarkeit.

### 26.3.2 3.2 Klassifizierungsstufen

Die Organisation verwendet folgende Klassifizierungsstufen: - **Öffentlich (Public):** Informationen, die öffentlich zugänglich sind oder sein dürfen - **Intern (Internal):** Informationen für den internen Gebrauch, nicht für die Öffentlichkeit bestimmt - **Vertraulich (Confidential):** Sensible Informationen, deren Offenlegung der Organisation schaden könnte - **Streng Vertraulich (Highly Confidential):** Hochsensible Informationen mit höchstem Schutzbedarf

### 26.3.3 3.3 Kennzeichnung und Labeling

Klassifizierte Informationen werden entsprechend gekennzeichnet: - Digitale Dokumente: Metadaten, Header/Footer, Wasserzeichen - Physische Dokumente: Stempel, Aufkleber, Deckblätter - E-Mails: Subject-Präfix, Banner - Speichermedien: Etiketten

### 26.3.4 3.4 Handling-Anforderungen

Für jede Klassifizierungsstufe gelten spezifische Handling-Anforderungen: - Zugriffskontrolle und Berechtigungen - Verschlüsselung (at rest, in transit) - Speicherung und Archivierung - Übertragung und Weitergabe - Vernichtung und Löschung

### 26.3.5 3.5 Information Owner Verantwortung

Jede Information hat einen definierten Information Owner, der verantwortlich ist für: - Klassifizierung der Information - Definition von Zugriffsrechten - Regelmäßige Überprüfung der Klassifizierung - Genehmigung von Zugriffs- und Weitergabeanfragen

### 26.3.6 3.6 Weitergabe und Sharing

Die Weitergabe klassifizierter Informationen erfolgt nur nach dem Need-to-Know-Prinzip: - Interne Weitergabe: Nach Genehmigung durch Information Owner - Externe Weitergabe: Nach Genehmigung und mit geeigneten Schutzmaßnahmen (NDA, Verschlüsselung) - Cloud-Speicherung: Nur in genehmigten Cloud-Services mit angemessenen Sicherheitskontrollen

### 26.3.7 3.7 Sichere Vernichtung

Informationen werden am Ende ihres Lebenszyklus sicher vernichtet: - Digitale Daten: Sichere Löschung (Overwriting, Degaussing) - Physische Dokumente: Schreddern, Verbrennen - Speichermedien: Physische Zerstörung bei hochsensiblen Daten

### 26.3.8 3.8 Datenschutz-Compliance

Die Klassifizierung und das Handling personenbezogener Daten erfolgt in Übereinstimmung mit der DSGVO und anderen Datenschutzvorschriften.

## 26.4 4. Rollen und Verantwortlichkeiten

### 26.4.1 RACI-Matrix: Datenklassifizierung und Informationshandling

Aktivität	CISO	Information Owner	Mitarbeiter	IT-Betrieb	Data Protection Officer
Policy-Erstellung	R/A	C	I	C	C
Klassifizierung	C	R/A	I	I	C
Kennzeichnung	A	R	C	I	
Zugriffsgenehmigung	R/A	I	I	C	
Handling-Compliance	A	R	R	C	C
Weitergabe-Genehmigung	C	R/A	I	I	C
Sichere Vernichtung	C	A	I	R	C
Monitoring und Audits	R/A	C	I	C	C

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

### 26.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **Information Owner:** Fachbereichsleiter, Systemverantwortliche
- **Data Protection Officer:** {{ meta.dpo.name }}
- **Umsetzungsverantwortliche:** Alle Mitarbeiter, IT-Betrieb
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit, DPO

## 26.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

### 26.5.1 Zugehörige Richtlinien

- **0290\_Richtlinie\_Datenklassifizierung\_Labeling\_und\_Handling.md** - Detaillierte Implementierungsrichtlinie
- **0260\_Policy\_Kryptografie\_und\_Schluesselmanagement.md** - Cryptography Policy

- 0560\_Policy\_Datenschutz\_Schnittstellen.md - Data Protection Policy
- 0580\_Policy\_Aufbewahrung\_und\_Loeschung.md - Retention and Deletion Policy

### 26.5.2 Zugehörige Standards/Baselins

- Klassifizierungsschema und Handling-Matrix
- Labeling-Standards (digital und physisch)
- Verschlüsselungsanforderungen pro Klassifizierungsstufe
- Vernichtungsstandards

### 26.5.3 Zugehörige Prozesse

- Klassifizierungsprozess
- Information Owner Assignment
- Weitergabe- und Sharing-Genehmigungsprozess
- Sichere Vernichtungsprozess

## 26.6 6. Compliance, Monitoring und Durchsetzung

### 26.6.1 Messgrößen und KPIs

- Anteil klassifizierter Informationen (Ziel: 100%)
- Anteil korrekt gekennzeichneter Dokumente
- Anzahl Verstöße gegen Handling-Anforderungen
- Anzahl unbefugter Weitergaben
- Durchschnittliche Zeit zur Klassifizierung neuer Informationen
- Compliance-Rate mit Vernichtungsanforderungen

### 26.6.2 Nachweise und Evidence

- Klassifizierungs-Register
- Information Owner Assignments
- Weitergabe-Genehmigungen
- Vernichtungsnachweise
- DLP (Data Loss Prevention) Logs
- Audit-Berichte zu Klassifizierung und Handling

### 26.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:

- **Fehlende Klassifizierung:** Nachschulung, Korrektur - **Falsche Kennzeichnung:** Korrektur, Nachschulung
- **Unbefugte Weitergabe:** Verwarnung bis Kündigung, ggf. rechtliche Schritte
- **Unsachgemäße Vernichtung:** Untersuchung, Nachschulung
- **Wiederholte Verstöße:** Arbeitrechtliche Konsequenzen

## 26.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und Information Owner genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet und werden regelmäßig überprüft
- **Kompensationsmaßnahmen:** Ausnahmen erfordern alternative Sicherheitsmaßnahmen

## 26.8 8. Referenzen

### 26.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0290\_Richtlinie\_Datenklassifizierung\_Labeling\_und\_Handling.md - Detailed Guideline
- 0300\_Policy\_Asset\_Management.md - Asset Management Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

### 26.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.5.12 - Classification of information
- ISO/IEC 27001:2022 Annex A.5.13 - Labelling of information
- ISO/IEC 27001:2022 Annex A.5.14 - Information transfer
- ISO/IEC 27002:2022 - Information security controls
- DSGVO (EU 2016/679) - Datenschutz-Grundverordnung
- BSI IT-Grundschutz - Baustein CON.6 Löschen und Vernichten

**Genehmigt durch:**

{}{{ meta.management.ceo }}, Geschäftsführung  
Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 27

## Richtlinie: Datenklassifizierung, Labeling und Handling

**Dokument-ID:** 0290

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.12, A.5.13

**Owner:** {{ meta.it\_operations.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 27.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md und definiert:  
- Klassifizierungsstufen und Kriterien  
- Labeling-Verfahren für Dokumente und E-Mails  
- Handling-Anforderungen pro Klassifizierungsstufe

**Geltungsbereich:** Alle Informationen bei AdminSend GmbH

### 27.2 2. Klassifizierungsstufen

#### 27.2.1 2.1 Öffentlich (Public)

**Definition:** Informationen für öffentliche Verbreitung bestimmt

**Beispiele:** - Marketing-Materialien, Pressemitteilungen - Öffentliche Website-Inhalte - Produktdokumentationen

**Handling:** - Keine Zugriffsbeschränkungen - Keine Verschlüsselung erforderlich - Freie Weitergabe erlaubt

## **27.2.2 2.2 Intern (Internal)**

**Definition:** Informationen für interne Nutzung, nicht für Öffentlichkeit

**Beispiele:** - Interne Prozessdokumentationen - Organisationsstrukturen - Allgemeine Geschäftskommunikation

**Handling:** - Zugriff nur für Mitarbeiter und autorisierte Dritte - Keine Verschlüsselung erforderlich (außer bei externer Übertragung) - Weitergabe an Dritte nur mit NDA

## **27.2.3 2.3 Vertraulich (Confidential)**

**Definition:** Sensible Geschäftsinformationen, Schaden bei Offenlegung

**Beispiele:** - Verträge, Angebote - Personaldaten - Finanzberichte (intern) - Kundendaten

**Handling:** - Zugriff nur nach Need-to-Know-Prinzip - Verschlüsselung bei Übertragung und Speicherung - Weitergabe nur mit Genehmigung - Sichere Vernichtung erforderlich

## **27.2.4 2.4 Streng Vertraulich (Highly Confidential)**

**Definition:** Höchst sensible Informationen, erheblicher Schaden bei Offenlegung

**Beispiele:** - Geschäftsgeheimnisse, M&A-Pläne - Strategische Pläne - Sicherheitskonzepte - Kritische Infrastrukturdaten

**Handling:** - Zugriff nur für autorisierte Personen (explizite Genehmigung) - Verschlüsselung verpflichtend (at rest und in transit) - Keine E-Mail-Versand ohne Verschlüsselung - Physische Dokumente in Safe - Sichere Vernichtung nach DIN 66399 P-5

# **27.3 3. Klassifizierungsprozess**

## **27.3.1 3.1 Verantwortlichkeiten**

**Daten-Owner:** - Klassifizierung neuer Informationen - Review und Anpassung bei Änderungen - Genehmigung von Zugriffen

**Ersteller:** - Anwendung der Klassifizierung bei Dokumenterstellung - Labeling gemäß Vorgaben - Einhaltung Handling-Anforderungen

**IT-Betrieb:** - Technische Umsetzung (DLP, Verschlüsselung) - Monitoring und Compliance-Checks

## **27.3.2 3.2 Klassifizierungskriterien**

**Fragen zur Bestimmung:** 1. Welcher Schaden entsteht bei Offenlegung? 2. Gibt es gesetzliche/regulatorische Anforderungen? 3. Wer benötigt Zugriff (Öffentlichkeit, Mitarbeiter, spezifische Personen)? 4. Wie lange müssen Daten aufbewahrt werden?

**Entscheidungsbaum:** - Öffentlich bestimmt? → Öffentlich - Nur intern relevant? → Intern - Geschäftsschaden bei Offenlegung? → Vertraulich - Erheblicher Schaden oder gesetzliche Pflicht? → Streng Vertraulich

## 27.4 4. Labeling-Verfahren

### 27.4.1 4.1 Dokumente

**Microsoft Office:** - Sensitivity Labels in Office 365 - Automatische Anwendung über DLP-Regeln  
- Header/Footer mit Klassifizierung

**PDF:** - Wasserzeichen mit Klassifizierung - Metadaten-Tags

**Physische Dokumente:** - Stempel oder Aufdruck auf jeder Seite - Farbcodierung (z.B. Rot für Streng Vertraulich)

### 27.4.2 4.2 E-Mails

**Betreffzeile:** - Präfix: [VERTRAULICH], [STRENG VERTRAULICH] - Automatisch durch E-Mail-Client

**E-Mail-Body:** - Disclaimer im Footer - Verschlüsselung bei Vertraulich/Streng Vertraulich

**Outlook-Integration:** - Sensitivity Labels - Automatische Verschlüsselung bei Klassifizierung

### 27.4.3 4.3 Digitale Assets

**Dateisysteme:** - Metadaten-Tags - Separate Ordnerstrukturen pro Klassifizierung - Zugriffskontrolle über ACLs

**Datenbanken:** - Spalten-Level-Klassifizierung - Row-Level-Security - Audit-Logging für Zugriffe

## 27.5 5. Handling-Anforderungen

### 27.5.1 5.1 Speicherung

Klassifizierung	Speicherort	Verschlüsselung	Zugriffskontrolle
Öffentlich	Beliebig	Optional	Keine
Intern	Genehmigte Systeme	Bei externer Speicherung	Mitarbeiter
Vertraulich	Genehmigte Systeme	Verpflichtend	Need-to-Know
Streng Vertraulich	Dedizierte Systeme	Verpflichtend (AES-256)	Explizite Genehmigung

### 27.5.2 5.2 Übertragung

Klassifizierung	E-Mail	Dateitransfer	Physisch
Öffentlich	Unverschlüsselt	Beliebig	Keine Anforderungen
Intern	OK TLS empfohlen	SFTP/HTTPS	Versiegelte Umschläge

Klassifizierung	E-Mail	Dateitraffic	Physisch
Vertraulich	S/MIME verpflichtend	SFTP/HTTPS verschlüsselt	Einschreiben, versiegelt
Streng Vertraulich	S/MIME + Genehmigung	Dedizierte Kanäle	Kurier, persönliche Übergabe

### 27.5.3 5.3 Vernichtung

Klassifizierung	Digital	Papier	Datenträger
Öffentlich	Normale Lösung	Papierkorb	Normale Lösung
Intern	Sichere Lösung	Shredder P-3	Sichere Lösung
Vertraulich	Kryptographische Lösung	Shredder P-4	Degaussing + Zerstörung
Streng Vertraulich	Kryptographische Lösung	Shredder P-5	Physische Zerstörung

## 27.6 6. Data Loss Prevention (DLP)

### 27.6.1 6.1 DLP-Regeln

**Automatische Erkennung:** - Kreditkartenzahlen, Sozialversicherungsnummern - Dokumente mit "Vertraulich"-Label - Personenbezogene Daten (DSGVO)

**Aktionen:** - **Warnung:** Bei Versand Intern-klassifizierter Daten extern - **Blockierung:** Bei Versand Vertraulich/Streng Vertraulich ohne Verschlüsselung - **Quarantäne:** Bei Verdacht auf Datenleck

### 27.6.2 6.2 Monitoring

**Überwachte Kanäle:** - E-Mail (ausgehend) - Cloud-Uploads (OneDrive, SharePoint) - USB-Geräte - Drucker

**Alerts:** - Automatische Benachrichtigung an Security-Team - Incident-Erstellung bei kritischen Verstößen

## 27.7 7. Schulung und Awareness

**Pflichtschulungen:** - Onboarding: Datenklassifizierung-Grundlagen - Jährlich: Refresher und Updates

**Awareness-Materialien:** - Poster mit Klassifizierungsstufen - Quick-Reference-Karten - Intranet-Artikel

## 27.8 8. Compliance und Audit

### 27.8.1 8.1 Messgrößen (KPIs)

Metrik	Zielwert
Klassifizierte Dokumente	> 80%
DLP-Incidents	< 10 pro Monat
Schulungsteilnahme	100%

### 27.8.2 8.2 Audit-Nachweise

- Klassifizierungs-Register
- DLP-Logs und Incidents
- Schulungsnachweise
- Zugriffsprotokolle

## 27.9 9. Referenzen

### 27.9.1 Interne Dokumente

- 0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md
- 0320\_PolicyLogging\_und\_Monitoring.md

### 27.9.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.5.12 - Classification of information
- ISO/IEC 27001:2022 Annex A.5.13 - Labelling of information
- DIN 66399 - Vernichtung von Datenträgern

---

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 28

## Policy: Asset Management

**Dokument-ID:** 0300

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.9-A.5.11 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 28.1 1. Zweck

Diese Policy definiert die Grundsätze für Asset Management und Inventarverwaltung der **Admin-Send GmbH**. Sie stellt sicher, dass alle Informationswerte (Assets) identifiziert, dokumentiert, klassifiziert und über ihren gesamten Lebenszyklus angemessen geschützt werden.

### 28.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Asset-Typen:** Hardware, Software, Daten, Informationen, Dienste, Personen, immaterielle Werte
- **Systeme:** Alle IT-Systeme, Netzwerkkomponenten, Endgeräte, Server, Cloud-Ressourcen
- **Lebenszyklus:** Beschaffung, Inbetriebnahme, Betrieb, Wartung, Außerbetriebnahme, Entsorgung
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_) zulässig.

## **28.3 3. Grundsätze (Policy Statements)**

### **28.3.1 3.1 Vollständiges Asset-Inventar**

Alle Assets der Organisation werden in einem zentralen Asset-Inventar erfasst und dokumentiert. Das Inventar wird regelmäßig aktualisiert und auf Vollständigkeit überprüft.

### **28.3.2 3.2 Asset Owner Assignment**

Jedes Asset hat einen definierten Asset Owner, der verantwortlich ist für: - Klassifizierung des Assets - Definition von Schutzanforderungen - Genehmigung von Zugriffs- und Nutzungsrechten - Lifecycle-Management

### **28.3.3 3.3 Asset-Klassifizierung und Tagging**

Assets werden klassifiziert und mit Metadaten versehen (Tagging): - Klassifizierung nach Schutzbedarf (Vertraulichkeit, Integrität, Verfügbarkeit) - Technische Tags (Umgebung, Applikation, Kostenstelle) - Compliance-Tags (DSGVO, PCI-DSS, etc.)

### **28.3.4 3.4 Lifecycle-Management**

Assets werden über ihren gesamten Lebenszyklus verwaltet: - **Beschaffung:** Sicherheitsanforderungen, Genehmigungsprozess - **Inbetriebnahme:** Konfiguration, Härtung, Dokumentation - **Betrieb:** Wartung, Patching, Monitoring - **Außerbetriebnahme:** Datenlöschung, Dekommissionierung - **Entsorgung:** Sichere Vernichtung, Recycling

### **28.3.5 3.5 Akzeptable Nutzung**

Assets dürfen nur für genehmigte geschäftliche Zwecke genutzt werden. Private Nutzung ist nur im Rahmen der Acceptable Use Policy (0200\_Policy\_Akzeptable\_Nutzung\_IT.md) gestattet.

### **28.3.6 3.6 Rückgabe von Assets**

Bei Rollenwechsel oder Austritt müssen alle Assets zurückgegeben werden. Der Rückgabeprozess ist Teil des Leaver-Prozesses.

### **28.3.7 3.7 Schutz vor Verlust und Diebstahl**

Assets werden durch geeignete Maßnahmen vor Verlust, Diebstahl und unbefugtem Zugriff geschützt: - Physische Sicherheit (Zutrittskontrolle, Alarmanlagen) - Verschlüsselung mobiler Geräte - Remote-Wipe-Funktionalität - Versicherung kritischer Assets

### **28.3.8 3.8 Sichere Entsorgung**

Assets werden am Ende ihres Lebenszyklus sicher entsorgt: - Datenlöschung nach anerkannten Standards - Physische Zerstörung bei hochsensiblen Daten - Umweltgerechtes Recycling - Dokumentation der Entsorgung

## 28.4 4. Rollen und Verantwortlichkeiten

### 28.4.1 RACI-Matrix: Asset Management

Aktivität	CISO	Asset Owner	IT-Betrieb	Procurement	Facility Management
Policy-Erstellung	R/A	C	C	C	I
Asset-Inventarisierung	A	R	R	C	C
Asset-Owner	C	R/A	I	I	I
Assignment					
Klassifizierung	C	R/A	I	I	I
Lifecycle-Management	A	R	R	C	C
Sichere Entsorgung	C	A	R	I	R
Monitoring und Audits	R/A	C	C	I	I

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

### 28.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **Asset Owner:** Fachbereichsleiter, Systemverantwortliche
- **Asset Manager:** {{ meta.it.asset\_manager }}
- **Umsetzungsverantwortliche:** IT-Betrieb, Procurement, Facility Management
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit

## 28.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

### 28.5.1 Zugehörige Richtlinien

- **0310\_Richtlinie\_Asset\_Inventory\_Tagging\_und\_Entsorgung.md** - Detaillierte Implementierungsrichtlinie
- **0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md** - Data Classification Policy
- **0200\_Policy\_Akzeptable\_Nutzung\_IT.md** - Acceptable Use Policy
- **0480\_Policy\_Physische\_Sicherheit.md** - Physical Security Policy

### 28.5.2 Zugehörige Standards/Baselinses

- Asset-Inventar-Schema (CMDB)

- Tagging-Standards
- Entsorgungsstandards
- Lifecycle-Management-Prozesse

### 28.5.3 Zugehörige Prozesse

- Asset-Beschaffungsprozess
- Asset-Onboarding und Konfiguration
- Asset-Rückgabeprozess (Leaver)
- Sichere Entsorgungsprozess

## 28.6 6. Compliance, Monitoring und Durchsetzung

### 28.6.1 Messgrößen und KPIs

- Inventarisierungsrate (Ziel: 100% aller Assets erfasst)
- Anzahl Assets ohne Asset Owner
- Anzahl nicht klassifizierter Assets
- Durchschnittliche Zeit zur Asset-Registrierung
- Anzahl verlorener oder gestohlener Assets
- Compliance-Rate mit Entsorgungsstandards

### 28.6.2 Nachweise und Evidence

- Asset-Inventar (CMDB)
- Asset Owner Assignments
- Klassifizierungs-Register
- Entsorgungsnachweise
- Audit-Berichte zu Asset Management
- Versicherungsnachweise

### 28.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:

- **Nicht registrierte Assets:** Nachregistrierung, Nachschulung - **Verlust von Assets:** Untersuchung, ggf. Kostenerstattung - **Unsachgemäße Entsorgung:** Nachschulung, Disziplinarmaßnahmen - **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen

## 28.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und Asset Owner genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet

## 28.8 8. Referenzen

### 28.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0310\_Richtlinie\_Asset\_Inventory\_Tagging\_und\_Entsorgung.md - Detailed Guideline
- 0720\_Anhang\_Asset\_und\_Systeminventar\_Template.md - Asset Inventory Template
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

### 28.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.5.9 - Inventory of information and other associated assets
  - ISO/IEC 27001:2022 Annex A.5.10 - Acceptable use of information and other associated assets
  - ISO/IEC 27001:2022 Annex A.5.11 - Return of assets
  - ISO/IEC 27002:2022 - Information security controls
  - ITIL 4 - IT Asset Management
  - ISO/IEC 19770 - IT Asset Management
- 

**Genehmigt durch:**

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 29

## Richtlinie: Asset Inventory, Tagging und Entsorgung

**Dokument-ID:** 0310

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0300\_Policy\_Asset\_Management.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.9, A.5.10

**Owner:** {{ meta.it\_operations.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 29.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0300\_Policy\_Asset\_Management.md und definiert: - Asset-Inventarisierung und CMDB-Verwaltung - Asset-Tagging und Kennzeichnung - Lifecycle-Management und Entsorgung

**Geltungsbereich:** Alle IT-Assets bei AdminSend GmbH

### 29.2 2. Asset-Kategorien

#### 29.2.1 2.1 Hardware-Assets

- Laptops, Desktops, Server
- Netzwerkgeräte (Switches, Router, Firewalls)
- Mobilgeräte (Smartphones, Tablets)
- Peripherie (Monitore, Drucker, Scanner)
- Speichermedien (USB-Sticks, externe Festplatten)

## 29.2.2 2.2 Software-Assets

- Betriebssysteme und Lizenzen
- Anwendungssoftware
- Cloud-Subscriptions (SaaS)
- Entwicklungstools

## 29.2.3 2.3 Informations-Assets

- Datenbanken
- Dateisysteme und Shares
- Dokumentensammlungen
- Backup-Medien

## 29.2.4 2.4 Services

- Cloud-Services (IaaS, PaaS, SaaS)
- Managed Services
- Support-Verträge

## 29.3 3. Asset-Inventarisierung

### 29.3.1 3.1 CMDB (Configuration Management Database)

**System:** {{ meta.itsm.cmdb }} (z.B. ServiceNow, Jira Service Management)

**Pflichtfelder pro Asset:** - Asset-ID (einzigartig) - Asset-Typ und Kategorie - Hersteller, Modell, Seriennummer - Standort, Raum - Owner, Nutzer - Anschaffungsdatum, Kosten - Wartungsvertrag, Support-Ende - Status (In Betrieb, Lager, Defekt, Entsorgt)

**Zusatzfelder:** - IP-Adresse, MAC-Adresse (Netzwerkgeräte) - Betriebssystem, Patch-Level - Installierte Software - Klassifizierung (Kritikalität) - Abhängigkeiten zu anderen Assets

### 29.3.2 3.2 Automatische Inventarisierung

**Tools:** - **Endpoint-Management:** {{ meta.endpoint.management }} (z.B. Microsoft Intune, Jamf) - **Network Discovery:** {{ meta.network.discovery }} (z.B. Nmap, Lansweeper) - **Cloud Asset Inventory:** Native Cloud-Tools (Azure Resource Graph, AWS Config)

**Prozess:** - Tägliche automatische Scans - Abgleich mit CMDB - Alerts bei unbekannten Assets (Shadow IT) - Automatische Aktualisierung von Attributen

### 29.3.3 3.3 Manuelle Inventarisierung

**Anlässe:** - Neue Asset-Beschaffung - Asset-Übergabe an Mitarbeiter - Standortwechsel - Wartung oder Reparatur - Außerbetriebnahme

**Prozess:** 1. Asset physisch prüfen 2. CMDB-Eintrag erstellen/aktualisieren 3. Asset-Tag anbringen 4. Dokumentation (Fotos bei Bedarf) 5. Übergabeprotokoll (bei Mitarbeiter-Zuweisung)

## 29.4 4. Asset-Tagging

### 29.4.1 4.1 Tagging-Schema

**Asset-ID-Format:** {{ meta.asset.id\_format }}

Beispiel: LAP-2024-001234 (Laptop, Jahr, laufende Nummer)

**Präfixe:** - LAP: Laptop - DSK: Desktop - SRV: Server - NET: Netzwerkgerät - MOB: Mobilgerät  
- PER: Peripherie

### 29.4.2 4.2 Physische Tags

**Barcode/QR-Code-Labels:** - Selbstklebend, manipulationssicher - Anbringung an sichtbarer Stelle - Enthält Asset-ID und QR-Code für CMDB-Link

**RFID-Tags (optional):** - Für hochwertige Assets - Automatische Erfassung bei Standortwechsel  
- Integration mit Zutrittskontrollsysten

### 29.4.3 4.3 Digitale Tags

**Hostname-Konvention:** - Format: {{ meta.naming.hostname\_format }} - Beispiel: lap-jdoe-001 (Typ-Nutzer-Nummer)

**Metadaten:** - Cloud-Resources: Tags für Owner, Kostenstelle, Umgebung - Virtuelle Maschinen: Tags für Anwendung, Kritikalität

## 29.5 5. Asset-Lifecycle-Management

### 29.5.1 5.1 Beschaffung

**Prozess:** 1. Bedarfsanforderung über Ticketsystem 2. Genehmigung durch Vorgesetzten und IT-Leitung 3. Beschaffung über genehmigte Lieferanten 4. Wareneingang und Qualitätsprüfung 5. CMDB-Eintrag erstellen 6. Asset-Tag anbringen 7. Bereitstellung an Nutzer

**Dokumentation:** - Bestellung, Rechnung - Garantie- und Wartungsverträge - Übergabeprotokoll

### 29.5.2 5.2 Betrieb

**Wartung:** - Regelmäßige Wartung gemäß Herstellervorgaben - Dokumentation in CMDB - Firmware- und Software-Updates

**Monitoring:** - Hardware-Health-Checks - Kapazitätsplanung - Lebenszyklusende-Tracking

### 29.5.3 5.3 Außerbetriebnahme

**Trigger:** - Ende der Nutzungsdauer (typisch 3-5 Jahre) - Defekt, nicht reparabel - Technologiewechsel - Mitarbeiter-Offboarding

**Prozess:** 1. Asset aus Betrieb nehmen 2. Daten sichern (falls erforderlich) 3. Daten sicher löschen (siehe Abschnitt 6) 4. CMDB-Status auf "Außer Betrieb" setzen 5. Entscheidung: Wiederverwendung, Verkauf oder Entsorgung

## 29.6 6. Sichere Datenvernichtung

### 29.6.1 6.1 Datenträger-Lösung

Methoden nach DIN 66399:

Datenträger	Klassifizierung	Methode	Standard
HDD	Intern	Software-Lösung (3-Pass)	DIN 66399 H-3
HDD	Vertraulich	Degaussing + Lösung	DIN 66399 H-4
HDD	Streng Vertraulich	Physische Zerstörung	DIN 66399 H-5
SSD	Intern	Secure Erase (ATA)	DIN 66399 H-3
SSD	Vertraulich/Streng Vertraulich	Kryptographische Lösung + Zerstörung	DIN 66399 H-5
USB/SD	Alle	Physische Zerstörung	DIN 66399 H-4

**Tools:** - **Software:** DBAN, Blancco, Parted Magic - **Hardware:** Degausser, Shredder

**Dokumentation:** - Löschprotokoll mit Asset-ID, Datum, Methode, Durchführender - Zertifikat bei Dienstleister-Entsorgung

### 29.6.2 6.2 Mobile Geräte

**Prozess:** 1. Remote Wipe über MDM ({{ meta.mdm.system }}) 2. Factory Reset vor Ort 3. Entfernung von SIM-Karten und SD-Karten 4. Physische Prüfung der Löschung 5. Dokumentation

### 29.6.3 6.3 Cloud-Daten

**Lösung:** - Logische Lösung in Cloud-Service - Warten auf Retention-Period-Ablauf - Bestätigung der endgültigen Lösung durch Provider - Dokumentation (Löschbestätigung)

## 29.7 7. Asset-Entsorgung

### 29.7.1 7.1 Wiederverwendung

**Intern:** - Aufbereitung und Neuinstallation - Zuweisung an anderen Mitarbeiter - Nutzung als Test- oder Entwicklungsgerät

**Spende:** - Datenvernichtung gemäß Abschnitt 6 - Entfernung aller Asset-Tags und Firmenlogos - Dokumentation der Spende (Steuer)

## 29.7.2 7.2 Verkauf

**Remarketing:** - Nur nach vollständiger Datenvernichtung - Verkauf über zertifizierte Remarketing-Partner - Erlös-Dokumentation

## 29.7.3 7.3 Entsorgung

**Zertifizierte Entsorgungspartner:** - WEEE-zertifiziert (Waste Electrical and Electronic Equipment) - Entsorgungsnachweis erforderlich - Umweltgerechte Entsorgung

**Prozess:** 1. Datenvernichtung (siehe Abschnitt 6) 2. Übergabe an Entsorgungspartner 3. Entsorgungsnachweis erhalten 4. CMDB-Status auf "Entsorgt" setzen 5. Dokumentation archivieren

# 29.8 8. Compliance und Audit

## 29.8.1 8.1 Messgrößen (KPIs)

Metrik	Zielwert
CMDB-Vollständigkeit	> 95%
Asset-Tagging-Rate	100%
Inventur-Abweichungen	< 2%
Entsorgungsnachweise	100%

## 29.8.2 8.2 Regelmäßige Inventuren

**Frequenz:** - Vollständige Inventur: Jährlich - Stichproben: Quartalsweise - Ad-hoc bei Verdacht auf Verlust

**Prozess:** 1. CMDB-Export 2. Physische Prüfung vor Ort 3. Abgleich CMDB vs. Realität 4. Klärung von Abweichungen 5. CMDB-Korrektur 6. Bericht an Management

## 29.8.3 8.3 Audit-Nachweise

- CMDB-Berichte
- Asset-Übergabeprotokolle
- Löschprotokolle
- Entsorgungsnachweise
- Inventur-Berichte

# 29.9 9. Referenzen

## 29.9.1 Interne Dokumente

- 0300\_Policy\_Asset\_Management.md
- 0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md

## 29.9.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.5.9 - Inventory of information and other associated assets
  - ISO/IEC 27001:2022 Annex A.5.10 - Acceptable use of information
  - DIN 66399 - Vernichtung von Datenträgern
  - WEEE-Richtlinie - Elektro- und Elektronikgeräte-Entsorgung
- 

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 30

## Policy: Logging und Monitoring

**Dokument-ID:** 0320

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.8.15, A.8.16 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 30.1 1. Zweck

Diese Policy definiert die Grundsätze für Logging, Monitoring und Security Event Management der **AdminSend GmbH**. Sie stellt sicher, dass sicherheitsrelevante Ereignisse erfasst, überwacht und analysiert werden, um Sicherheitsvorfälle zu erkennen, zu untersuchen und darauf zu reagieren.

### 30.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Systeme:** Alle IT-Systeme, Anwendungen, Netzwerkkomponenten, Sicherheitssysteme
- **Log-Quellen:** Server, Workstations, Netzwerkgeräte, Firewalls, IDS/IPS, Anwendungen, Datenbanken
- **Monitoring-Bereiche:** Sicherheit, Performance, Verfügbarkeit, Compliance
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_zulässig).

### **30.3 3. Grundsätze (Policy Statements)**

#### **30.3.1 3.1 Umfassendes Logging**

Alle sicherheitsrelevanten Ereignisse werden protokolliert: - Authentisierungsversuche (erfolgreich und fehlgeschlagen) - Zugriffe auf sensible Daten und Systeme - Privilegierte Aktivitäten (Admin-Zugriffe, Konfigurationsänderungen) - Sicherheitsvorfälle und Anomalien - System- und Anwendungsfehler

#### **30.3.2 3.2 Zentralisiertes Log-Management**

Logs werden zentral in einem SIEM (Security Information and Event Management) System gesammelt, gespeichert und analysiert. Dies ermöglicht korrelierte Analysen und effiziente Incident Response.

#### **30.3.3 3.3 Log-Integrität und Schutz**

Logs werden vor unbefugter Änderung und Löschung geschützt: - Schreibgeschützte Log-Speicherung - Integritätsprüfungen (Hashing, digitale Signaturen) - Zugriffskontrolle auf Log-Systeme - Verschlüsselte Übertragung

#### **30.3.4 3.4 Retention und Aufbewahrung**

Logs werden entsprechend gesetzlicher, regulatorischer und geschäftlicher Anforderungen aufbewahrt: - Sicherheitslogs: Mindestens 12 Monate online, 7 Jahre Archiv - Audit-Logs: Entsprechend Compliance-Anforderungen - Performance-Logs: Entsprechend Betriebsanforderungen

#### **30.3.5 3.5 Proaktives Monitoring und Alerting**

Sicherheitsrelevante Ereignisse werden proaktiv überwacht und bei Anomalien werden Alerts generiert: - Real-time Monitoring kritischer Systeme - Automatisierte Alerting-Regeln - Eskalationsprozesse für kritische Alerts - 24/7 SOC (Security Operations Center) für kritische Systeme

#### **30.3.6 3.6 SIEM Use Cases und Detection Rules**

SIEM-Systeme werden mit Use Cases und Detection Rules konfiguriert, um bekannte Angriffsmuster und Anomalien zu erkennen: - Brute-Force-Angriffe - Privilege Escalation - Data Exfiltration - Malware-Aktivitäten - Insider-Threats

#### **30.3.7 3.7 Log-Analyse und Forensik**

Logs werden regelmäßig analysiert und bei Sicherheitsvorfällen für forensische Untersuchungen genutzt: - Regelmäßige Log-Reviews - Threat Hunting - Incident Investigation - Root Cause Analysis

#### **30.3.8 3.8 Datenschutz-Compliance**

Logging und Monitoring erfolgen in Übereinstimmung mit Datenschutzvorschriften (DSGVO): - Minimierung personenbezogener Daten in Logs - Zweckbindung der Log-Daten - Zugriffskontrolle auf personenbezogene Log-Daten - Löschung nach Ablauf der Retention-Periode

## 30.4 4. Rollen und Verantwortlichkeiten

### 30.4.1 RACI-Matrix: Logging und Monitoring

Aktivität	CISO	SOC/Security Operations	IT-Betrieb	System Owner	DPO
Policy-Erstellung	R/A	C	C	C	C
SIEM-Betrieb	A	R	C	I	I
Log-Konfiguration	C	C	R	R	I
Monitoring und Alerting	A	R	C	I	I
Incident Investigation	A	R	C	C	C
Log-Retention	C	C	R	I	C
Compliance-Prüfung	R/A	C	C	I	C

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

### 30.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **SOC Manager:** {{ meta.security.soc\_manager }}
- **SIEM Administrator:** {{ meta.it.siem\_admin }}
- **Umsetzungsverantwortliche:** SOC, IT-Betrieb, System Owner
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit, DPO

## 30.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

### 30.5.1 Zugehörige Richtlinien

- **0330\_RichtlinieLogging\_SIEM\_und\_Audit\_Trails.md** - Detaillierte Implementierungsrichtlinie
- **0400\_Policy\_Incident\_Management.md** - Incident Management Policy
- **0560\_Policy\_Datenschutz\_Schnittstellen.md** - Data Protection Policy
- **0340\_Policy\_Vulnerability\_und\_Patch\_Management.md** - Vulnerability Management Policy

### 30.5.2 Zugehörige Standards/Baselinses

- Log-Standards und Formate

- SIEM Use Cases und Detection Rules
- Retention-Anforderungen
- Alerting-Schwellwerte

### 30.5.3 Zugehörige Prozesse

- Log-Onboarding-Prozess
- Alert-Triage und Eskalation
- Incident Investigation
- Log-Review-Prozess

## 30.6 6. Compliance, Monitoring und Durchsetzung

### 30.6.1 Messgrößen und KPIs

- Anzahl Log-Quellen im SIEM (Ziel: 100% kritischer Systeme)
- Log-Vollständigkeit und -Verfügbarkeit (Ziel: 99.9%)
- Durchschnittliche Zeit zur Alert-Triage (MTTD - Mean Time To Detect)
- Anzahl False Positives pro Tag
- SIEM Use Case Coverage
- Compliance-Rate mit Retention-Anforderungen

### 30.6.2 Nachweise und Evidence

- SIEM-Konfiguration und Use Cases
- Log-Retention-Nachweise
- Alert-Statistiken und Triage-Reports
- Incident Investigation Reports
- Audit-Berichte zu Logging und Monitoring
- Datenschutz-Impact-Assessments

### 30.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:

- **Deaktivierung von Logging:** Sofortige Remediation, Untersuchung
- **Unbefugte Log-Manipulation:** Incident Response, arbeitsrechtliche Konsequenzen
- **Nicht-Compliance mit Retention:** Remediation, Nachschulung
- **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen

## 30.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet
- **Kompensationsmaßnahmen:** Ausnahmen erfordern alternative Sicherheitsmaßnahmen

## 30.8 8. Referenzen

### 30.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0330\_RichtlinieLogging\_SIEM\_und\_Audit\_Trails.md - Detailed Guideline
- 0400\_Policy\_Incident\_Management.md - Incident Management Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

### 30.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.8.15 - Logging
- ISO/IEC 27001:2022 Annex A.8.16 - Monitoring activities
- ISO/IEC 27002:2022 - Information security controls
- NIST SP 800-92 - Guide to Computer Security Log Management
- DSGVO (EU 2016/679) - Datenschutz-Grundverordnung
- BSI IT-Grundschutz - Baustein OPS.1.1.5 Protokollierung

---

**Genehmigt durch:**

{}{{ meta.management.ceo }}, Geschäftsführung

Datum: {}{{ meta.document.approval\_date }}

**Nächster Review:** {}{{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 31

## Richtlinie: Logging, SIEM und Audit Trails

**Dokument-ID:** 0330

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0320\_Policy\_Logging\_und\_Monitoring.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.8.15, A.8.16

**Owner:** {{ meta.it\_operations.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Vertraulich

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 31.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0320\_Policy\_Logging\_und\_Monitoring.md und definiert:

- Logging-Anforderungen pro System-Typ - SIEM-Integration und Use Cases - Audit-Trail-Anforderungen und Retention

**Geltungsbereich:** Alle IT-Systeme bei AdminSend GmbH

### 31.2 2. Logging-Anforderungen

#### 31.2.1 2.1 Zu protokollierende Events

**Authentifizierung:** - Erfolgreiche und fehlgeschlagene Logins - Logout-Events - MFA-Challenges und -Ergebnisse - Passwort-Änderungen und -Resets - Account-Sperrungen und -Entsperrungen

**Autorisierung:** - Zugriffe auf vertrauliche Daten - Privilegierte Operationen (sudo, Admin-Rechte) - Zugriffsverweigerungen (Access Denied) - Änderungen an Berechtigungen

**System-Events:** - System-Start und -Shutdown - Service-Starts und -Stops - Konfigurationsänderungen - Software-Installationen und -Updates - Fehler und Exceptions

**Daten-Events:** - Datei-Zugriffe (Lesen, Schreiben, Löschen) - Datenbank-Queries (bei sensiblen Daten) - Daten-Exporte und -Downloads - Backup-Operationen

**Netzwerk-Events:** - Firewall-Blocks und -Allows - VPN-Verbindungen - Netzwerk-Scans - Anomalien im Traffic

### 31.2.2 2.2 Log-Format und Inhalte

**Pflichtfelder:** - Timestamp (UTC, ISO 8601) - Event-Typ und Severity - Quelle (System, Anwendung, IP) - Nutzer/Account - Aktion/Operation - Ergebnis (Erfolg/Fehler) - Zusätzliche Kontextinformationen

Beispiel (JSON):

```
{  
    "timestamp": "2024-02-02T10:15:30Z",  
    "event_type": "authentication",  
    "severity": "info",  
    "source_ip": "192.168.1.100",  
    "user": "jdoe",  
    "action": "login",  
    "result": "success",  
    "mfa_method": "authenticator_app"  
}
```

### 31.2.3 2.3 Logging-Level

System-Typ	Logging-Level	Begründung
Produktionssysteme	INFO	Balance zwischen Detail und Performance
Entwicklungssysteme	DEBUG	Fehlersuche
Sicherheitssysteme (Firewall, IDS)	VERBOSE	Maximale Sichtbarkeit
Privilegierte Systeme	VERBOSE	Compliance und Forensik

## 31.3 3. SIEM-Integration

### 31.3.1 3.1 SIEM-System

**Plattform:** {{ meta.security.siem\_solution }} (z.B. Splunk, Microsoft Sentinel, Elastic SIEM)

**Architektur:** - Log-Sammlung über Agents oder Syslog - Zentrale Log-Aggregation - Normalisierung und Enrichment - Korrelation und Alerting - Langzeit-Archivierung

### 31.3.2 3.2 Log-Quellen

**Priorität 1 (Kritisch):** - Active Directory / Azure AD - Firewalls und IDS/IPS - VPN-Gateways - Privilegierte Access Management (PAM) - Datenbanken mit vertraulichen Daten

**Priorität 2 (Hoch):** - Web-Server und Application-Server - E-Mail-Gateways - Cloud-Services (Azure, AWS, Google Cloud) - Endpoint Detection and Response (EDR)

**Priorität 3 (Mittel):** - Workstations und Laptops - Netzwerk-Switches - Drucker und IoT-Geräte

### 31.3.3 3.3 SIEM Use Cases

**Authentifizierung:** - Brute-Force-Angriffe (> 10 fehlgeschlagene Logins in 5 Minuten) - Unmögliche Reisen (Logins von geografisch unmöglichen Standorten) - Privilegierte Account-Nutzung außerhalb Geschäftszeiten

**Malware und Intrusion:** - Malware-Detektionen durch EDR - IDS/IPS-Alerts - Command & Control (C2) Kommunikation - Lateral Movement (ungewöhnliche interne Verbindungen)

**Data Exfiltration:** - Große Datenmengen-Uploads zu externen Zielen - Zugriff auf viele vertrauliche Dateien in kurzer Zeit - Ungewöhnliche Datenbank-Queries

**Compliance:** - Zugriffe auf PII (Personally Identifiable Information) - Änderungen an Sicherheitskonfigurationen - Privilegierte Operationen ohne Genehmigung

### 31.3.4 3.4 Alerting und Response

**Severity-Level:** - **Critical:** Sofortige Eskalation an On-Call Security (24/7) - **High:** Eskalation innerhalb 1 Stunde - **Medium:** Bearbeitung innerhalb 4 Stunden - **Low:** Bearbeitung innerhalb 1 Arbeitstag

**Automatische Response:** - Account-Sperrung bei Brute-Force - IP-Blockierung bei Malware-C2 - Quarantäne von Endpoints bei Malware-Detektion

## 31.4 4. Audit Trails

### 31.4.1 4.1 Anforderungen

**Unveränderlichkeit:** - Logs dürfen nicht nachträglich geändert werden - Kryptographische Signaturen oder Write-Once-Storage - Zugriff auf Logs nur für autorisierte Personen

**Vollständigkeit:** - Lückenlose Aufzeichnung aller relevanten Events - Monitoring der Log-Integrität - Alerts bei Log-Ausfällen

**Nachvollziehbarkeit:** - Wer hat was wann gemacht? - Rekonstruktion von Ereignisketten - Forensische Analyse möglich

### 31.4.2 4.2 Privilegierte Zugriffe

**Zusätzliche Anforderungen:** - Session-Recording für privilegierte Zugriffe - Vier-Augen-Prinzip bei kritischen Operationen - Genehmigungsworkflow vor Zugriff - Detaillierte Protokollierung aller Aktionen

**PAM-Integration:** - Privileged Access Management System: {{ meta.security.pam\_solution }} - Just-in-Time (JIT) Access - Automatische Passwort-Rotation - Session-Monitoring und -Recording

### 31.4.3 4.3 Compliance-Audit-Trails

**Regulatorische Anforderungen:** - DSGVO: Zugriffe auf personenbezogene Daten - SOX: Finanzrelevante Transaktionen - HIPAA: Zugriffe auf Gesundheitsdaten (falls zutreffend)

**Dokumentation:** - Wer hat auf welche Daten zugegriffen? - Zweck des Zugriffs - Genehmigung (falls erforderlich) - Zeitraum

## 31.5 5. Log-Retention

### 31.5.1 5.1 Aufbewahrungsfristen

Log-Typ	Retention (Online)	Retention (Archiv)	Begründung
Security-Logs	90 Tage	<code>meta.retention.log_years</code> } } Jahre	Forensik, Compliance
Authentifizierung Logs	90 Tage	<code>meta.retention.log_years</code> } } Jahre	Audit, Compliance
System-Logs	30 Tage	1 Jahr	Troubleshooting
Application-Logs	30 Tage	1 Jahr	Debugging
Audit-Trails (Compliance)	180 Tage	<code>meta.retention.audit_years</code> } } Jahre	Regulatorisch

### 31.5.2 5.2 Archivierung

**Prozess:** 1. Logs älter als Retention-Period (Online) werden archiviert 2. Komprimierung und Verschlüsselung 3. Übertragung zu Archiv-Storage (z.B. Azure Blob Archive, AWS Glacier) 4. Verifizierung der Archivierung 5. Löschung aus Online-SIEM

**Zugriff auf Archiv:** - Nur bei begründetem Bedarf (Forensik, Audit) - Genehmigung durch CISO  
- Wiederherstellung in SIEM für Analyse

### 31.5.3 5.3 Sichere Löschung

**Nach Ablauf der Retention:** - Automatische Löschung aus Archiv - Kryptographische Löschung (Schlüssel vernichten) - Dokumentation der Löschung

## 31.6 6. Log-Sicherheit

### 31.6.1 6.1 Zugriffskontrolle

**Berechtigungen:** - **Security-Team:** Vollzugriff auf alle Logs - **IT-Betrieb:** Zugriff auf System- und Application-Logs - **Auditoren:** Read-Only-Zugriff auf Audit-Trails - **Entwickler:** Zugriff nur auf Dev-Logs

**Authentifizierung:** - MFA für SIEM-Zugriff - Privilegierte Accounts für Admin-Operationen - Audit-Logging für SIEM-Zugriffe

### 31.6.2 6.2 Verschlüsselung

**In Transit:** - TLS 1.2+ für Log-Übertragung - Mutual TLS für kritische Systeme

**At Rest:** - Verschlüsselung des SIEM-Storage (AES-256) - Verschlüsselung von Archiv-Logs

### **31.6.3 6.3 Integritätsschutz**

**Methoden:** - Kryptographische Signaturen (HMAC) - Write-Once-Read-Many (WORM) Storage  
- Blockchain-basierte Log-Integrität (optional)

**Monitoring:** - Regelmäßige Integritätsprüfungen - Alerts bei Manipulationsversuchen

## **31.7 7. Monitoring und Alerting**

### **31.7.1 7.1 Log-Health-Monitoring**

**Überwachte Metriken:** - Log-Ingestion-Rate (Logs pro Sekunde) - Log-Latenz (Zeit bis Log in SIEM)  
- Fehlende Log-Quellen - SIEM-Storage-Kapazität

**Alerts:** - Log-Quelle sendet keine Logs (> 15 Minuten) - Ungewöhnlich hohe Log-Rate (möglicher Angriff oder Fehler) - SIEM-Storage > 80% voll

### **31.7.2 7.2 Security-Monitoring**

**24/7 Security Operations Center (SOC):** - Monitoring aller SIEM-Alerts - Triage und Incident Response - Eskalation bei kritischen Incidents

**Automatisierung:** - SOAR (Security Orchestration, Automation and Response) - Automatische Playbooks für häufige Incidents - Integration mit Ticketsystem

## **31.8 8. Compliance und Audit**

### **31.8.1 8.1 Messgrößen (KPIs)**

Metrik	Zielwert
Log-Quellen-Verfügbarkeit	> 99%
SIEM-Alert-Response-Zeit (Critical)	< 15 Minuten
False-Positive-Rate	< 10%
Log-Retention-Compliance	100%

### **31.8.2 8.2 Audit-Nachweise**

- SIEM-Konfiguration und Use Cases
- Log-Retention-Berichte
- Incident-Response-Dokumentation
- Zugriffsprotokolle auf SIEM

## **31.9 9. Referenzen**

### **31.9.1 Interne Dokumente**

- 0320\_Policy\_Logging\_und\_Monitoring.md
- 0400\_Policy\_Incident\_Management.md

### 31.9.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.8.15 - Logging
  - ISO/IEC 27001:2022 Annex A.8.16 - Monitoring activities
  - NIST SP 800-92 - Guide to Computer Security Log Management
- 

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 32

## Policy: Vulnerability und Patch Management

**Dokument-ID:** 0340

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.8.8 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 32.1 1. Zweck

Diese Policy definiert die Grundsätze für Vulnerability und Patch Management der **AdminSend GmbH**. Sie stellt sicher, dass technische Schwachstellen zeitnah identifiziert, bewertet und behoben werden, um das Risiko von Sicherheitsvorfällen zu minimieren.

### 32.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Systeme:** Alle IT-Systeme, Anwendungen, Betriebssysteme, Netzwerkkomponenten, Firmware
- **Schwachstellentypen:** Software-Schwachstellen, Konfigurationsfehler, fehlende Patches
- **Umgebungen:** Produktion, Test, Entwicklung, Cloud, On-Premise
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_) zulässig.

## **32.3 3. Grundsätze (Policy Statements)**

### **32.3.1 3.1 Proaktive Schwachstellenidentifikation**

Schwachstellen werden proaktiv durch regelmäßige Vulnerability Scans, Penetration Tests und Security Assessments identifiziert.

### **32.3.2 3.2 Risikoorientierte Priorisierung**

Schwachstellen werden nach Risiko priorisiert (CVSS-Score, Exploitability, Auswirkung, Exposition). Kritische Schwachstellen haben höchste Priorität.

### **32.3.3 3.3 Zeitnahe Remediation**

Schwachstellen werden innerhalb definierter SLAs behoben: - **Kritisch (CVSS 9.0-10.0):** 7 Tage - **Hoch (CVSS 7.0-8.9):** 30 Tage - **Mittel (CVSS 4.0-6.9):** 90 Tage - **Niedrig (CVSS 0.1-3.9):** 180 Tage oder nach Risikobewertung

### **32.3.4 3.4 Patch Management Lifecycle**

Patches werden über einen strukturierten Prozess ausgerollt: - **Identifikation:** Überwachung von Vendor Security Bulletins - **Bewertung:** Risiko- und Impact-Analyse - **Test:** Validierung in Test-Umgebung - **Deployment:** Kontrolliertes Rollout in Produktion - **Verification:** Überprüfung der erfolgreichen Installation

### **32.3.5 3.5 Emergency Patching**

Für kritische Zero-Day-Schwachstellen oder aktiv ausgenutzte Exploits existiert ein beschleunigter Emergency-Patch-Prozess.

### **32.3.6 3.6 Kompensationsmaßnahmen**

Wenn Patches nicht sofort angewendet werden können, werden Kompensationsmaßnahmen implementiert (z.B. Netzwerksegmentierung, WAF-Regeln, IPS-Signaturen).

### **32.3.7 3.7 Vulnerability Disclosure**

Schwachstellen in eigenen Produkten oder Diensten werden verantwortungsvoll offengelegt (Responsible Disclosure).

### **32.3.8 3.8 Continuous Monitoring**

Systeme werden kontinuierlich auf neue Schwachstellen überwacht. Automatisierte Scanning-Tools werden eingesetzt.

## **32.4 4. Rollen und Verantwortlichkeiten**

### **32.4.1 RACI-Matrix: Vulnerability und Patch Management**

Aktivität	CISO	Vulnerability Manager	IT-Betrieb	System Owner	Change Management
Policy-Erstellung	R/A	C	C	C	I
Vulnerability Scanning		R	C	I	I
Schwachstellen-Auswertung	A	R	C	C	I
Patch-Test	C	C	R	R	I
Patch-Deployment	C	C	R	A	R
Emergency Patching	A	R	R	C	C
Monitoring und Reporting	A	R	C	I	I

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

### 32.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **Vulnerability Manager:** {{ meta.security.vuln\_manager }}
- **Patch Manager:** {{ meta.it.patch\_manager }}
- **Umsetzungsverantwortliche:** IT-Betrieb, System Owner
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit

## 32.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

### 32.5.1 Zugehörige Richtlinien

- **0350\_Richtlinie\_Vulnerability\_Scans\_Patching\_und\_Exploitation\_Response.md**  
- Detaillierte Implementierungsrichtlinie
- **0360\_Policy\_Change\_und\_Release\_Management.md** - Change Management Policy
- **0400\_Policy\_Incident\_Management.md** - Incident Management Policy
- **0540\_Policy\_Konfiguration\_und\_Hardening.md** - Configuration Management Policy

### 32.5.2 Zugehörige Standards/Baselinses

- Vulnerability Scanning Schedule
- Patch SLAs und Priorisierung
- Emergency Patch Prozess
- Kompensationsmaßnahmen-Katalog

### 32.5.3 Zugehörige Prozesse

- Vulnerability Management Prozess
- Patch Management Prozess
- Emergency Patch Prozess
- Penetration Testing Prozess

## 32.6 6. Compliance, Monitoring und Durchsetzung

### 32.6.1 Messgrößen und KPIs

- Anzahl offener Schwachstellen nach Severity
- Durchschnittliche Zeit zur Remediation (MTTR - Mean Time To Remediate)
- Patch-Compliance-Rate (Ziel: 95% innerhalb SLA)
- Anzahl überfälliger Patches
- Anzahl Emergency Patches pro Quartal
- Vulnerability Scan Coverage (Ziel: 100% kritischer Systeme)

### 32.6.2 Nachweise und Evidence

- Vulnerability Scan Reports
- Patch-Deployment-Logs
- Remediation-Nachweise
- Kompensationsmaßnahmen-Dokumentation
- Penetration Test Reports
- Audit-Berichte zu Patch-Compliance

### 32.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:

- **Nicht gepatchte kritische Systeme:** Sofortige Remediation, Untersuchung - **Überschreitung von SLAs:** Eskalation, Remediation-Plan - **Unbefugtes Patching:** Rollback, Nachschulung - **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen

## 32.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und System Owner genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet
- **Kompensationsmaßnahmen:** Ausnahmen erfordern alternative Sicherheitsmaßnahmen

## 32.8 8. Referenzen

### 32.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy

- 0350\_Richtlinie\_Vulnerability\_Scans\_Patching\_und\_Exploitation\_Response.md - Detailed Guideline
- 0360\_Policy\_Change\_und\_Release\_Management.md - Change Management Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

### 32.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.8.8 - Management of technical vulnerabilities
  - ISO/IEC 27002:2022 - Information security controls
  - NIST SP 800-40 - Guide to Enterprise Patch Management Technologies
  - CVSS v3.1 - Common Vulnerability Scoring System
  - CWE/SANS Top 25 - Most Dangerous Software Weaknesses
  - OWASP Top 10 - Web Application Security Risks
- 

**Genehmigt durch:**

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 33

## Richtlinie: Vulnerability Scans, Patching und Exploitation Response

**Dokument-ID:** 0350

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0340\_Policy\_Vulnerability\_und\_Patch\_Management.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.8.8

**Owner:** {{ meta.it\_operations.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 33.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0340\_Policy\_Vulnerability\_und\_Patch\_Management.md und definiert:  
- Vulnerability-Scanning-Prozesse und -Frequenzen  
- Patch-Management-Workflows  
- Exploitation-Response bei aktiv ausgenutzten Schwachstellen

**Geltungsbereich:** Alle IT-Systeme bei AdminSend GmbH

### 33.2 2. Vulnerability Scanning

#### 33.2.1 2.1 Scan-Typen

**Authenticated Scans:** - Mit Credentials, tiefere Analyse - Erkennung von Konfigurationsschwächen - Software-Inventar und Patch-Level

**Unauthenticated Scans:** - Ohne Credentials, Angreifer-Perspektive - Erkennung extern sichtbarer Schwachstellen - Netzwerk-Services und offene Ports

**Web Application Scans:** - OWASP Top 10 Schwachstellen - SQL-Injection, XSS, CSRF - API-Security-Tests

### 33.2.2 2.2 Scan-Frequenzen

System-Typ	Authenticated	Unauthenticated	Web App
Produktionssysteme	Wöchentlich	Monatlich	Monatlich
Entwicklungssysteme	Monatlich	Quartalsweise	Bei Deployment
Kritische Infrastruktur	Wöchentlich	Wöchentlich	Wöchentlich
Externe Systeme	N/A	Wöchentlich	Wöchentlich

**Ad-hoc-Scans:** - Nach neuen Systemen/Anwendungen - Nach kritischen Schwachstellen-Veröffentlichungen - Nach Sicherheitsvorfällen

### 33.2.3 2.3 Scanning-Tools

**Vulnerability Scanner:** {{ meta.security.vuln\_scanner }} (z.B. Tenable Nessus, Qualys, Rapid7)

**Web Application Scanner:** {{ meta.security.web\_scanner }} (z.B. Burp Suite, OWASP ZAP)

**Container Scanner:** {{ meta.security.container\_scanner }} (z.B. Trivy, Snyk)

### 33.2.4 2.4 Scan-Prozess

1. **Planung:** Scan-Zeitfenster festlegen (außerhalb Geschäftszeiten)
2. **Durchführung:** Automatisierte Scans
3. **Analyse:** Review der Ergebnisse durch Security-Team
4. **Priorisierung:** Schwachstellen nach Severity und Exploitability
5. **Remediation:** Ticketerstellung für IT-Betrieb
6. **Verification:** Re-Scan nach Behebung

## 33.3 3. Schwachstellen-Bewertung

### 33.3.1 3.1 Severity-Klassifizierung

**CVSS-Score (Common Vulnerability Scoring System):** - **Critical (9.0-10.0):** Sofortige Behebung erforderlich - **High (7.0-8.9):** Behebung innerhalb 7 Tage - **Medium (4.0-6.9):** Behebung innerhalb 30 Tage - **Low (0.1-3.9):** Behebung innerhalb 90 Tage

### 33.3.2 3.2 Priorisierung

**Faktoren:** - CVSS-Score - Exploitability (Exploit verfügbar?) - Asset-Kritikalität - Exposition (Internet-facing?) - Kompensationskontrollen vorhanden?

**Priorisierungs-Matrix:** | CVSS | Internet-facing | Exploit verfügbar | Priorität | SLA | |——|—  
|——|——|——| | Critical | Ja | Ja | P1 | 24 Stunden | | Critical | Ja | Nein |  
P1 | 48 Stunden | | Critical | Nein | Ja | P2 | 7 Tage | | High | Ja | Ja | P2 | 7 Tage | | High | Nein |  
Nein | P3 | 30 Tage |

### 33.3.3 3.3 False Positives

**Prozess:** - Security-Team prüft Schwachstelle - Bei False Positive: Markierung im Scanner - Dokumentation der Begründung - Regelmäßiger Review (quartalsweise)

## 33.4 4. Patch Management

### 33.4.1 4.1 Patch-Quellen

**Betriebssysteme:** - Windows: WSUS / Windows Update - Linux: Paketmanager (apt, yum, dnf)  
- macOS: Software Update

**Anwendungen:** - Hersteller-Updates - Third-Party-Patch-Management (z.B. Ninite, Chocolatey)

**Firmware:** - Hersteller-Portale - Automatische Update-Checks

### 33.4.2 4.2 Patch-Prozess

**Phase 1: Patch-Identifikation** - Automatische Benachrichtigungen von Herstellern - Vulnerability-Scan-Ergebnisse - Security-Advisories (CVE, CERT)

**Phase 2: Bewertung und Priorisierung** - Relevanz für eigene Systeme prüfen - Severity und Exploitability bewerten - Priorisierung gemäß Abschnitt 3.2

**Phase 3: Testing** - Test in Dev/Test-Umgebung - Kompatibilitätsprüfung - Rollback-Plan erstellen

**Phase 4: Deployment** - Staging: Pilotgruppe (10% der Systeme) - Monitoring auf Probleme (24 Stunden) - Rollout: Restliche Systeme - Verifizierung: Patch erfolgreich installiert?

**Phase 5: Verification** - Re-Scan zur Bestätigung der Behebung - Dokumentation im Ticketsystem

### 33.4.3 4.3 Patch-Zeitfenster

**Wartungsfenster:** - **Produktionssysteme:** Sonntag 02:00-06:00 Uhr - **Entwicklungssysteme:** Täglich außerhalb Geschäftszeiten - **Kritische Patches:** Notfall-Wartungsfenster nach Bedarf

**Automatisches Patching:** - Workstations: Automatisch, außerhalb Geschäftszeiten - Server: Manuell nach Testing - Kritische Systeme: Change-Genehmigung erforderlich

### 33.4.4 4.4 Emergency Patching

**Trigger:** - Aktiv ausgenutzter Exploit (Zero-Day) - Kritische Schwachstelle in Internet-facing System - Ransomware-Kampagne

**Prozess:** 1. **Sofortige Bewertung:** Betroffene Systeme identifizieren 2. **Notfall-Change:** Beschleunigte Genehmigung 3. **Minimales Testing:** Nur kritische Funktionen testen 4. **Sofortiges Deployment:** Innerhalb 24 Stunden 5. **Monitoring:** Erhöhtes Monitoring nach Patch

## 33.5 5. Exploitation Response

### 33.5.1 5.1 Threat Intelligence

**Quellen:** - **CISA KEV (Known Exploited Vulnerabilities):** <https://www.cisa.gov/known-exploited-vulnerabilities-catalog> - **CERT-Bund:** <https://www.cert-bund.de/> - **Vendor Security Advisories - Threat Intelligence Feeds:** {{ meta.security.threat\_intel }}

**Monitoring:** - Tägliche Prüfung auf neue Exploits - Automatische Alerts bei kritischen Schwachstellen - Abgleich mit eigenen Systemen

### 33.5.2 5.2 Zero-Day-Response

**Prozess:** 1. **Detektion:** Threat Intelligence oder IDS/IPS-Alert 2. **Bewertung:** Betroffene Systeme identifizieren 3. **Containment:** Sofortmaßnahmen zur Risikominimierung 4. **Mitigation:** Workarounds oder Kompensationskontrollen 5. **Patching:** Sobald Patch verfügbar 6. **Lessons Learned:** Post-Incident-Review

**Sofortmaßnahmen (Containment):** - Netzwerk-Segmentierung (Firewall-Regeln) - Deaktivierung betroffener Services - IDS/IPS-Signaturen aktualisieren - Erhöhtes Monitoring

### 33.5.3 5.3 Kompensationskontrollen

**Wenn Patching nicht sofort möglich:** - **Netzwerk-Isolation:** Betroffene Systeme isolieren - **WAF-Regeln:** Web Application Firewall-Regeln - **IPS-Signaturen:** Intrusion Prevention System - **Zugriffsbeschränkungen:** Nur autorisierte Nutzer - **Erhöhtes Monitoring:** SIEM-Alerts für Exploitation-Versuche

**Dokumentation:** - Begründung für verzögertes Patching - Implementierte Kompensationskontakte - Risikobewertung - Geplantes Patch-Datum

## 33.6 6. Vulnerability Disclosure

### 33.6.1 6.1 Responsible Disclosure

**Prozess für externe Researcher:** 1. **Meldung:** security@{{ meta.organization.domain }} 2. **Bestätigung:** Innerhalb 24 Stunden 3. **Bewertung:** Innerhalb 7 Tage 4. **Remediation:** Gemäß Severity-SLA 5. **Disclosure:** Koordiniert mit Researcher (90 Tage)

**Bug Bounty Program (optional):** - Plattform: {{ meta.security.bug\_bounty }} (z.B. HackerOne, Bugcrowd) - Scope: Definierte Systeme und Anwendungen - Rewards: Nach Severity

### 33.6.2 6.2 Vendor Disclosure

**Bei Schwachstellen in Vendor-Produkten:** 1. Meldung an Vendor 2. Koordination mit Vendor für Patch 3. Keine öffentliche Disclosure vor Patch-Verfügbarkeit 4. Implementierung von Workarounds

## 33.7 7. Compliance und Audit

### 33.7.1 7.1 Messgrößen (KPIs)

Metrik	Zielwert
Critical Patches (SLA-Einhaltung)	> 95%
Scan-Coverage	100% aller Systeme
Mean Time to Patch (Critical)	< 7 Tage
Open Critical Vulnerabilities	< 5

### **33.7.2 7.2 Reporting**

**Monatlicher Vulnerability Report:** - Anzahl Schwachstellen nach Severity - Patch-Compliance-Rate - SLA-Verstöße - Trend-Analyse

**Quartalsweiser Management-Report:** - Vulnerability-Posture - Risiko-Entwicklung - Verbesserungsmaßnahmen

### **33.7.3 7.3 Audit-Nachweise**

- Scan-Berichte und -Historie
- Patch-Deployment-Logs
- Remediation-Tickets
- Kompensationskontrollen-Dokumentation

## **33.8 8. Referenzen**

### **33.8.1 Interne Dokumente**

- 0340\_Policy\_Vulnerability\_und\_Patch\_Management.md
- 0400\_Policy\_Incident\_Management.md

### **33.8.2 Externe Standards**

- ISO/IEC 27001:2022 Annex A.8.8 - Management of technical vulnerabilities
- NIST SP 800-40 - Guide to Enterprise Patch Management
- CVSS v3.1 - Common Vulnerability Scoring System

---

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 34

## Policy: Change und Release Management

**Dokument-ID:** 0360

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.8.32 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 34.1 1. Zweck

Diese Policy definiert die Grundsätze für Change und Release Management der **AdminSend GmbH**. Sie stellt sicher, dass Änderungen an IT-Systemen kontrolliert, getestet und dokumentiert werden, um Betriebsunterbrechungen und Sicherheitsrisiken zu minimieren.

### 34.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Systeme:** Alle IT-Systeme, Anwendungen, Infrastruktur, Netzwerke, Cloud-Services
- **Change-Typen:** Standard Changes, Normal Changes, Emergency Changes
- **Umgebungen:** Produktion, Test, Entwicklung
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_) zulässig.

### **34.3 3. Grundsätze (Policy Statements)**

#### **34.3.1 3.1 Kontrollierte Änderungen**

Alle Änderungen an produktiven IT-Systemen müssen über den Change Management Prozess genehmigt, dokumentiert und nachverfolgt werden.

#### **34.3.2 3.2 Change-Kategorisierung**

Changes werden nach Risiko und Auswirkung kategorisiert: - **Standard Changes:** Vorab genehmigte, risikoarme, wiederkehrende Changes - **Normal Changes:** Reguläre Changes mit CAB-Genehmigung - **Emergency Changes:** Dringende Changes zur Behebung kritischer Probleme

#### **34.3.3 3.3 Change Advisory Board (CAB)**

Ein Change Advisory Board bewertet und genehmigt Normal und Emergency Changes. Das CAB besteht aus Vertretern von IT, Security, Business und Change Management.

#### **34.3.4 3.4 Risiko- und Impact-Analyse**

Vor jeder Änderung wird eine Risiko- und Impact-Analyse durchgeführt. Sicherheitsrisiken werden bewertet und Mitigationsmaßnahmen definiert.

#### **34.3.5 3.5 Test und Validierung**

Changes werden in Test-Umgebungen validiert, bevor sie in Produktion ausgerollt werden. Kritische Changes erfordern umfassende Tests.

#### **34.3.6 3.6 Rollback-Planung**

Für jeden Change existiert ein Rollback-Plan, um bei Problemen schnell zum vorherigen Zustand zurückkehren zu können.

#### **34.3.7 3.7 Dokumentation und Nachvollziehbarkeit**

Alle Changes werden dokumentiert (Beschreibung, Begründung, Genehmigung, Durchführung, Ergebnis). Changes sind nachvollziehbar und auditierbar.

#### **34.3.8 3.8 Security Review**

Changes mit Sicherheitsrelevanz erfordern ein Security Review durch das Security Team vor der Genehmigung.

### **34.4 4. Rollen und Verantwortlichkeiten**

#### **34.4.1 RACI-Matrix: Change und Release Management**

Aktivität	Change Manager	CAB	CISO	Change Requester	IT-Betrieb
Policy-Erstellung	C	C	R/A	I	C
Change-Antrag	I	I	I	R	I
Risiko-Analyse	R	C	C	C	C
CAB-Genehmigung	R	A	C	I	I
Security Review	C	C	R/A	I	I
Change-Durchführung	C	I	I	I	R/A
Rollback	R	I	C	I	R/A
Post-Implementation	R/A	C	C	C	C
Review					

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

### 34.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **Change Manager:** {{ meta.it.change\_manager }}
- **CAB Chair:** {{ meta.it.cab\_chair }}
- **Umsetzungsverantwortliche:** IT-Betrieb, Entwicklung
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit

## 34.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

### 34.5.1 Zugehörige Richtlinien

- **0370\_Richtlinie\_Change\_Management\_mit\_Sicherheitsfreigaben.md** - Detaillierte Implementierungsrichtlinie
- **0340\_Policy\_Vulnerability\_und\_Patch\_Management.md** - Patch Management Policy
- **0380\_Policy\_Secure\_Development.md** - Secure Development Policy
- **0400\_Policy\_Incident\_Management.md** - Incident Management Policy

### 34.5.2 Zugehörige Standards/Baselinses

- Change-Kategorisierung und Genehmigungsprozesse
- CAB-Zusammensetzung und Entscheidungskriterien
- Test- und Validierungsanforderungen
- Rollback-Prozeduren

### 34.5.3 Zugehörige Prozesse

- Change Management Prozess
- Emergency Change Prozess
- Release Management Prozess
- Post-Implementation Review

## 34.6 6. Compliance, Monitoring und Durchsetzung

### 34.6.1 Messgrößen und KPIs

- Anzahl Changes pro Kategorie (Standard, Normal, Emergency)
- Change Success Rate (Ziel: >95%)
- Anzahl Failed Changes und Rollbacks
- Durchschnittliche Change-Durchlaufzeit
- Anzahl ungenehmigter Changes (Ziel: 0)
- Security Review Coverage für sicherheitsrelevante Changes (Ziel: 100%)

### 34.6.2 Nachweise und Evidence

- Change-Tickets und Genehmigungen
- CAB-Meeting-Protokolle
- Security Review Dokumentation
- Test-Ergebnisse
- Rollback-Dokumentation
- Post-Implementation Review Reports

### 34.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt: - **Ungenehmigter Change:** Rollback, Untersuchung, Nachschulung - **Fehlende Dokumentation:** Nachholung, Verwarnung - **Übersprungener Security Review:** Untersuchung, Disziplinarmaßnahmen - **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen

## 34.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom Change Manager und CISO genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden dokumentiert und im Post-Implementation Review besprochen
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet

## 34.8 8. Referenzen

### 34.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy

- 0370\_Richtlinie\_Change\_Management\_mit\_Sicherheitsfreigaben.md - Detailed Guideline
- 0340\_Policy\_Vulnerability\_und\_Patch\_Management.md - Patch Management Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

#### 34.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.8.32 - Change management
  - ISO/IEC 27002:2022 - Information security controls
  - ITIL 4 - Change Enablement
  - ISO/IEC 20000 - IT Service Management
- 

**Genehmigt durch:**

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 35

## Richtlinie: Change Management mit Sicherheitsfreigaben

**Dokument-ID:** 0370

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0360\_Policy\_Change\_und\_Release\_Management.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.8.32

**Owner:** {{ meta.it\_operations.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 35.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0360\_Policy\_Change\_und\_Release\_Management.md und definiert:  
- Change-Management-Prozesse mit Sicherheitsprüfungen  
- Change-Kategorien und Genehmigungsworkflows  
- Rollback-Verfahren und Post-Implementation-Reviews

**Geltungsbereich:** Alle IT-Änderungen bei AdminSend GmbH

### 35.2 2. Change-Kategorien

#### 35.2.1 2.1 Standard Changes

**Definition:** Vorab genehmigte, risikoarme, häufige Änderungen

**Beispiele:** - Passwort-Resets - Software-Updates (getestet) - Hinzufügen von Nutzern zu Standardgruppen

**Genehmigung:** Keine individuelle Genehmigung erforderlich

**Sicherheitsprüfung:** Nicht erforderlich

### 35.2.2 2.2 Normal Changes

**Definition:** Geplante Änderungen mit mittlerem Risiko

**Beispiele:** - Konfigurationsänderungen - Software-Installationen - Netzwerk-Änderungen

**Genehmigung:** Change Advisory Board (CAB)

**Sicherheitsprüfung:** Bei sicherheitsrelevanten Änderungen

### 35.2.3 2.3 Emergency Changes

**Definition:** Ungeplante, dringende Änderungen

**Beispiele:** - Kritische Security-Patches - Systemausfälle - Aktive Sicherheitsvorfälle

**Genehmigung:** Emergency CAB (ECAB)

**Sicherheitsprüfung:** Nachträglich

## 35.3 3. Change-Management-Prozess

### 35.3.1 3.1 Change Request (RFC)

**Pflichtfelder:** - Change-Titel und Beschreibung - Begründung (Business Justification) - Betroffene Systeme und Services - Risikobewertung - Rollback-Plan - Test-Ergebnisse - Geplantes Zeitfenster

**Sicherheitsrelevante Zusatzfelder:** - Auswirkungen auf Sicherheitskontrollen - Änderungen an Firewall-Regeln - Neue externe Verbindungen - Privilegierte Zugriffe erforderlich

### 35.3.2 3.2 Risikobewertung

**Risiko-Matrix:** | Wahrscheinlichkeit | Auswirkung Niedrig | Auswirkung Mittel | Auswirkung Hoch  
| |-----|-----|-----| | Niedrig | Niedrig | Niedrig | Mittel |  
| Mittel | Niedrig | Mittel | Hoch | | Hoch | Mittel | Hoch | Kritisch |

**Auswirkungen:** - **Niedrig:** Einzelter Nutzer betroffen - **Mittel:** Abteilung betroffen - **Hoch:** Gesamte Organisation betroffen

### 35.3.3 3.3 Sicherheitsprüfung

**Trigger:** - Änderungen an Sicherheitssystemen (Firewall, IDS, etc.) - Neue externe Verbindungen - Privilegierte Zugriffe - Änderungen an Authentifizierung/Autorisierung - Risiko "Hoch" oder "Kritisch"

**Prüfung durch IT-Security:** - Review des Change Requests - Sicherheitsauswirkungen bewerten - Zusätzliche Kontrollen empfehlen - Genehmigung oder Ablehnung

**SLA:** Sicherheitsprüfung innerhalb 2 Arbeitstagen

### 35.3.4 3.4 Change Advisory Board (CAB)

**Mitglieder:** - Change Manager (Vorsitz) - IT-Betrieb - IT-Security (bei sicherheitsrelevanten Changes) - Application Owner (bei Anwendungsänderungen) - Business Representative

**Frequenz:** Wöchentlich (Dienstag 10:00 Uhr)

**Aufgaben:** - Review und Genehmigung von Normal Changes - Priorisierung bei Konflikten - Risikobewertung - Terminplanung

### 35.3.5 3.5 Implementation

**Pre-Implementation:** - Backup erstellen - Rollback-Plan bereitstellen - Kommunikation an betroffene Nutzer - Monitoring vorbereiten

**Implementation:** - Änderung gemäß Plan durchführen - Dokumentation aller Schritte - Abweichungen dokumentieren

**Post-Implementation:** - Funktionstest - Monitoring auf Fehler (24 Stunden) - Change-Status aktualisieren - Dokumentation vervollständigen

### 35.3.6 3.6 Rollback

**Trigger:** - Funktionstest fehlgeschlagen - Kritische Fehler in Produktion - Sicherheitsprobleme erkannt

**Prozess:** 1. Rollback-Entscheidung durch Change Manager 2. Rollback gemäß Rollback-Plan 3. Verifizierung der Wiederherstellung 4. Root-Cause-Analyse 5. Neuer Change Request für erneuten Versuch

## 35.4 4. Emergency Changes

### 35.4.1 4.1 Emergency CAB (ECAB)

**Mitglieder:** - Change Manager oder Stellvertreter - IT-Betrieb (On-Call) - CISO oder IT-Security (On-Call)

**Verfügbarkeit:** 24/7

**Genehmigungsprozess:** - Telefonische oder E-Mail-Genehmigung - Dokumentation im Nachhinein - Review im nächsten regulären CAB

### 35.4.2 4.2 Emergency Change-Prozess

**Beschleunigter Workflow:** 1. **Initiierung:** Incident-Manager erstellt Emergency RFC 2. **Bewertung:** ECAB bewertet Dringlichkeit und Risiko 3. **Genehmigung:** ECAB genehmigt (oder lehnt ab) 4. **Implementation:** Sofortige Durchführung 5. **Dokumentation:** Nachträgliche Vervollständigung 6. **Review:** Im nächsten CAB

**Sicherheitsprüfung:** - Bei kritischen Security-Patches: Nachträglich - Bei anderen Emergency Changes: Vor Implementation (wenn möglich)

## 35.5 5. Sicherheitskontrollen

### 35.5.1 5.1 Segregation of Duties

**Prinzip:** Keine Person darf Change anfordern, genehmigen und implementieren

**Rollen:** - **Requester:** Beantragt Change - **Approver:** Genehmigt Change (CAB) - **Implementer:** Führt Change durch - **Reviewer:** Prüft Post-Implementation

### **35.5.2 5.2 Privilegierte Changes**

**Zusätzliche Anforderungen:** - Vier-Augen-Prinzip bei Implementation - Session-Recording - Detaillierte Dokumentation - Post-Implementation-Security-Review

### **35.5.3 5.3 Firewall-Changes**

**Spezielle Anforderungen:** - Begründung für jede neue Regel - Quell- und Ziel-IP/Port dokumentieren - Zeitliche Befristung (wo möglich) - Regelmäßiger Review (quartalsweise)

**Genehmigung:** - IT-Security: Verpflichtend - Network-Team: Technische Umsetzbarkeit - Application Owner: Business Justification

## **35.6 6. Testing und Validation**

### **35.6.1 6.1 Test-Umgebungen**

**Anforderungen:** - Dev/Test-Umgebung für alle kritischen Systeme - Möglichst identisch zu Produktion - Isoliert von Produktion

**Test-Prozess:** 1. Change in Dev/Test implementieren 2. Funktionstest durchführen 3. Performance-Test (bei Bedarf) 4. Security-Test (bei sicherheitsrelevanten Changes) 5. Dokumentation der Test-Ergebnisse

### **35.6.2 6.2 Security Testing**

**Bei sicherheitsrelevanten Changes:** - Vulnerability-Scan nach Change - Penetration-Test (bei kritischen Änderungen) - Code-Review (bei Software-Changes) - Configuration-Review

## **35.7 7. Dokumentation und Audit**

### **35.7.1 7.1 Change-Dokumentation**

**Pflicht-Dokumentation:** - Change Request (RFC) - Genehmigungen - Implementation-Log - Test-Ergebnisse - Post-Implementation-Review

**Aufbewahrung:** {{ meta.retention.change\_years }} Jahre

### **35.7.2 7.2 Post-Implementation Review (PIR)**

**Durchführung:** - Innerhalb 7 Tage nach Implementation - Bei allen Normal und Emergency Changes

**Inhalte:** - Erfolg der Implementation - Aufgetretene Probleme - Lessons Learned - Verbesserungsvorschläge

### **35.7.3 7.3 Compliance und Audit**

**Messgrößen (KPIs):** | Metrik | Zielwert | |————|————| | Erfolgreiche Changes | > 95% | | Emergency Changes | < 10% aller Changes | | Unauthorized Changes | 0 | | PIR-Completion-Rate | 100% |

**Audit-Nachweise:** - Change-Logs - Genehmigungen - Sicherheitsprüfungen - PIR-Berichte

## 35.8 8. Referenzen

### 35.8.1 Interne Dokumente

- 0360\_Policy\_Change\_und\_Release\_Management.md
- 0400\_Policy\_Incident\_Management.md

### 35.8.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.8.32 - Change management
- ITIL 4 - Change Enablement Practice

---

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 36

## Policy: Secure Development

**Dokument-ID:** 0380

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.8.25-A.8.28 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 36.1 1. Zweck

Diese Policy definiert die Grundsätze für sichere Softwareentwicklung (Secure SDLC) der **AdminSend GmbH**. Sie stellt sicher, dass Sicherheit in alle Phasen des Software Development Lifecycle integriert wird und Anwendungen sicher entwickelt, getestet und betrieben werden.

### 36.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Entwicklungsteams und Standorte der AdminSend GmbH
- **Anwendungen:** Alle intern entwickelten Anwendungen, APIs, Microservices, Mobile Apps
- **Entwicklungsphasen:** Requirements, Design, Implementation, Testing, Deployment, Maintenance
- **Entwicklungsmodelle:** Agile, Waterfall, DevOps, DevSecOps
- **Standorte:** {{ netbox.site.name }} und alle weiteren Entwicklungsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_zulässig).

## **36.3 3. Grundsätze (Policy Statements)**

### **36.3.1 3.1 Security by Design**

Sicherheit wird von Anfang an in den Entwicklungsprozess integriert (Shift Left). Sicherheitsanforderungen werden in der Requirements-Phase definiert und im Design berücksichtigt.

### **36.3.2 3.2 Secure Coding Standards**

Entwickler folgen anerkannten Secure Coding Standards (OWASP, CERT, CWE). Code wird nach Best Practices entwickelt, um häufige Schwachstellen zu vermeiden.

### **36.3.3 3.3 Code Reviews und Peer Reviews**

Alle Code-Änderungen durchlaufen Code Reviews. Sicherheitsrelevanter Code erfordert zusätzliche Security Reviews durch das Security Team.

### **36.3.4 3.4 Automatisierte Security Testing**

Security Testing ist in die CI/CD-Pipeline integriert: - **SAST (Static Application Security Testing)**: Statische Code-Analyse - **DAST (Dynamic Application Security Testing)**: Dynamische Sicherheitstests - **SCA (Software Composition Analysis)**: Analyse von Abhängigkeiten und Open-Source-Komponenten - **Container Scanning**: Sicherheitsprüfung von Container-Images

### **36.3.5 3.5 Secrets Management**

Secrets (Passwörter, API-Keys, Zertifikate) werden niemals im Code oder in Repositories gespeichert. Secrets werden in dedizierten Secrets Management Systemen verwaltet.

### **36.3.6 3.6 Dependency Management**

Externe Bibliotheken und Abhängigkeiten werden auf bekannte Schwachstellen überprüft. Veraltete oder unsichere Abhängigkeiten werden zeitnah aktualisiert.

### **36.3.7 3.7 Security Testing vor Produktionsfreigabe**

Vor der Produktionsfreigabe werden umfassende Sicherheitstests durchgeführt: - Penetration Testing für kritische Anwendungen - Security Acceptance Testing - Vulnerability Assessment

### **36.3.8 3.8 Secure Deployment und Configuration**

Anwendungen werden mit sicheren Konfigurationen deployed. Default-Credentials werden geändert, unnötige Features deaktiviert, Hardening-Maßnahmen angewendet.

## **36.4 4. Rollen und Verantwortlichkeiten**

### **36.4.1 RACI-Matrix: Secure Development**

Aktivität	CISO	Security Champion	Entwickler	DevOps	Security Team
Policy-Erstellung	R/A	C	C	C	C
Security Requirements	C	R	C	I	R/A
Secure Coding	I	C	R/A	I	C
Code Review	I	R	R	I	C
Security Review	A	C	I	I	R
AST/DAST/SCA Penetration Testing	C		I	R	R/A
Security Training	A	C	R	R	R

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

### 36.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **Security Champion:** Entwickler mit Security-Expertise in jedem Team
- **Application Security Lead:** {{ meta.security.appsec\_lead }}
- **Umsetzungsverantwortliche:** Entwickler, DevOps, Security Team
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit

## 36.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

### 36.5.1 Zugehörige Richtlinien

- **0390\_Richtlinie\_Secure\_SDLC\_Coding\_Review\_und\_Secrets.md** - Detaillierte Implementierungsrichtlinie
- **0360\_Policy\_Change\_und\_Release\_Management.md** - Change Management Policy
- **0340\_Policy\_Vulnerability\_und\_Patch\_Management.md** - Vulnerability Management Policy
- **0260\_Policy\_Kryptografie\_und\_Schluesselmanagement.md** - Cryptography Policy

### 36.5.2 Zugehörige Standards/Baselinses

- Secure Coding Standards (OWASP, CERT)
- Code Review Checklists
- SAST/DAST/SCA Tool-Konfigurationen
- Secrets Management Standards

### 36.5.3 Zugehörige Prozesse

- Secure SDLC Prozess
- Code Review Prozess
- Security Testing Prozess
- Vulnerability Disclosure Prozess

## 36.6 6. Compliance, Monitoring und Durchsetzung

### 36.6.1 Messgrößen und KPIs

- Anzahl Sicherheitsschwachstellen pro Release (Ziel: Reduktion um 50% jährlich)
- Code Review Coverage (Ziel: 100%)
- SAST/DAST/SCA Coverage (Ziel: 100% kritischer Anwendungen)
- Durchschnittliche Zeit zur Behebung von Schwachstellen (MTTR)
- Anzahl Secrets im Code (Ziel: 0)
- Security Training Completion Rate (Ziel: 100% jährlich)

### 36.6.2 Nachweise und Evidence

- Code Review Dokumentation
- SAST/DAST/SCA Reports
- Penetration Test Reports
- Security Acceptance Test Results
- Secrets Scanning Reports
- Security Training Nachweise

### 36.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt: -

**Secrets im Code:** Sofortige Rotation, Incident Response, Nachschulung - **Übersprungene Code Reviews:** Rollback, Nachholung, Verwarnung - **Ignorierte Security Findings:** Remediation, Nachschulung - **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen

## 36.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und Application Security Lead genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet
- **Kompensationsmaßnahmen:** Ausnahmen erfordern alternative Sicherheitsmaßnahmen

## 36.8 8. Referenzen

### 36.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy

- 0390\_Richtlinie\_Secure\_SDLC\_Coding\_Review\_und\_Secrets.md - Detailed Guideline
- 0360\_Policy\_Change\_und\_Release\_Management.md - Change Management Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

### 36.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.8.25 - Secure development lifecycle
  - ISO/IEC 27001:2022 Annex A.8.26 - Application security requirements
  - ISO/IEC 27001:2022 Annex A.8.27 - Secure system architecture and engineering principles
  - ISO/IEC 27001:2022 Annex A.8.28 - Secure coding
  - OWASP Top 10 - Web Application Security Risks
  - OWASP ASVS - Application Security Verification Standard
  - NIST SP 800-218 - Secure Software Development Framework (SSDF)
  - CWE Top 25 - Most Dangerous Software Weaknesses
- 

**Genehmigt durch:**

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 37

## Richtlinie: Secure SDLC, Code Reviews und Secrets Management

**Dokument-ID:** 0390

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0380\_Policy\_Secure\_Development.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.8.25, A.8.26

**Owner:** {{ meta.development.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 37.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0380\_Policy\_Secure\_Development.md und definiert: - Secure Software Development Lifecycle (SSDLC) - Code-Review-Prozesse und Security-Checks - Secrets Management und sichere Konfiguration

**Geltungsbereich:** Alle Softwareentwicklung bei **AdminSend GmbH**

### 37.2 2. Secure SDLC Phasen

#### 37.2.1 2.1 Requirements Phase

- Security Requirements definieren
- Threat Modeling durchführen
- Compliance-Anforderungen identifizieren

#### 37.2.2 2.2 Design Phase

- Security Architecture Review
- Data Flow Diagrams

- Authentication/Authorization-Design

### **37.2.3 2.3 Development Phase**

- Secure Coding Standards befolgen
- SAST (Static Application Security Testing)
- Dependency Scanning

### **37.2.4 2.4 Testing Phase**

- DAST (Dynamic Application Security Testing)
- Penetration Testing
- Security Test Cases

### **37.2.5 2.5 Deployment Phase**

- Security Configuration Review
- Secrets Management
- Deployment-Checkliste

### **37.2.6 2.6 Maintenance Phase**

- Vulnerability Management
- Security Patches
- Incident Response

## **37.3 3. Secure Coding Standards**

### **37.3.1 3.1 OWASP Top 10**

**Pflicht-Prävention:** 1. Broken Access Control 2. Cryptographic Failures 3. Injection 4. Insecure Design 5. Security Misconfiguration 6. Vulnerable Components 7. Authentication Failures 8. Software and Data Integrity Failures 9. Security Logging Failures 10. Server-Side Request Forgery (SSRF)

### **37.3.2 3.2 Input Validation**

- Alle Eingaben validieren (Whitelist-Ansatz)
- Parameterisierte Queries (SQL-Injection-Prävention)
- Output-Encoding (XSS-Prävention)

### **37.3.3 3.3 Authentication & Authorization**

- Keine eigene Krypto implementieren
- Etablierte Frameworks nutzen (OAuth 2.0, OpenID Connect)
- Least Privilege Principle

### **37.3.4 3.4 Error Handling**

- Keine sensitiven Informationen in Fehlermeldungen

- Zentrale Error-Logging
- Graceful Degradation

## 37.4 4. Code Reviews

### 37.4.1 4.1 Peer Code Review

**Prozess:** - Jeder Code-Change benötigt mindestens 1 Approval - Review vor Merge in Main Branch  
 - Checkliste für Security-Aspekte

**Security-Review-Checkliste:** - [ ] Input-Validierung vorhanden? - [ ] Keine Secrets im Code? -  
 [ ] Sichere Kryptografie verwendet? - [ ] Error-Handling korrekt? - [ ] Logging implementiert?

### 37.4.2 4.2 Security Champion Review

**Bei sicherheitskritischen Changes:** - Zusätzliches Review durch Security Champion - Security Champion: Entwickler mit Security-Training - Mindestens 1 Security Champion pro Team

### 37.4.3 4.3 Automated Code Review

**Tools:** - **SAST:** {{ meta.security.sast\_tool }} (z.B. SonarQube, Checkmarx) - **Dependency Check:** {{ meta.security.dependency\_tool }} (z.B. Snyk, Dependabot) - **Secrets Scanning:** {{ meta.security.secrets\_scanner }} (z.B. GitGuardian, TruffleHog)

**Integration:** - CI/CD-Pipeline - Automatische Scans bei jedem Commit - Blockierung bei Critical/High Findings

## 37.5 5. Secrets Management

### 37.5.1 5.1 Verbotene Praktiken

**Niemals:** - Secrets in Git committen - Secrets in Konfigurationsdateien (Klartext) - Secrets in Environment Variables (Produktion) - Secrets in Logs oder Error Messages

### 37.5.2 5.2 Secrets-Management-System

**System:** {{ meta.security.secrets\_manager }} (z.B. HashiCorp Vault, Azure Key Vault, AWS Secrets Manager)

**Funktionen:** - Zentrale Secrets-Speicherung (verschlüsselt) - Dynamische Secrets (kurzlebig) - Audit-Logging aller Zugriffe - Rotation von Secrets

### 37.5.3 5.3 Secrets-Rotation

**Frequenz:** - API-Keys: Alle 90 Tage - Database-Credentials: Alle 180 Tage - Service-Account-Passwords: Alle 180 Tage

**Automatisierung:** - Automatische Rotation wo möglich - Benachrichtigung vor Ablauf

### **37.5.4 5.4 Development vs. Production**

**Separate Secrets:** - Dev/Test: Separate Secrets (niedrigere Privilegien) - Produktion: Produktions-Secrets (höhere Privilegien) - Keine Wiederverwendung zwischen Umgebungen

## **37.6 6. Dependency Management**

### **37.6.1 6.1 Third-Party-Libraries**

**Anforderungen:** - Nur genehmigte Libraries verwenden - Regelmäßige Updates - Vulnerability-Scanning

**Genehmigungsprozess:** - Antrag über Ticketsystem - Security-Review der Library - Lizenz-Compliance-Prüfung - Genehmigung durch Security-Team

### **37.6.2 6.2 Software Composition Analysis (SCA)**

**Tools:** {{ meta.security.sca\_tool }} (z.B. Snyk, WhiteSource)

**Prozess:** - Automatisches Scanning bei Build - Identifikation bekannter Schwachstellen (CVEs) - Alerts bei kritischen Schwachstellen - Remediation-Empfehlungen

### **37.6.3 6.3 Dependency Updates**

**Strategie:** - Security-Updates: Sofort - Minor-Updates: Monatlich - Major-Updates: Nach Testing

## **37.7 7. CI/CD Security**

### **37.7.1 7.1 Pipeline Security**

**Security Gates:** 1. **Commit:** Secrets Scanning 2. **Build:** SAST, Dependency Check 3. **Test:** Unit Tests, Security Tests 4. **Deploy:** DAST, Configuration Review

**Blockierung bei:** - Critical/High SAST Findings - Known Exploited Vulnerabilities - Secrets im Code

### **37.7.2 7.2 Container Security**

**Image Scanning:** - Scan aller Container-Images - Nur signierte Images deployen - Regelmäßige Re-Scans

**Best Practices:** - Minimal Base Images - Non-Root User - Read-Only Filesystem

### **37.7.3 7.3 Infrastructure as Code (IaC)**

**Security Scanning:** - Terraform, CloudFormation, etc. - Tools: Checkov, Terrascan - Prüfung auf Misconfigurations

## 37.8 8. Security Testing

### 37.8.1 8.1 SAST (Static Application Security Testing)

**Frequenz:** Bei jedem Commit

**Tool:** {{ meta.security.sast\_tool }}

**Abdeckung:** Alle Programmiersprachen

### 37.8.2 8.2 DAST (Dynamic Application Security Testing)

**Frequenz:** Wöchentlich (Staging), vor jedem Release

**Tool:** {{ meta.security.dast\_tool }}

**Scope:** Web-Anwendungen, APIs

### 37.8.3 8.3 Penetration Testing

**Frequenz:** - Neue Anwendungen: Vor Go-Live - Bestehende Anwendungen: Jährlich - Nach kritischen Änderungen: Ad-hoc

**Durchführung:** - Intern oder externe Pentester - Scope-Definition - Remediation aller Findings - Re-Test nach Fixes

## 37.9 9. Compliance und Audit

### 37.9.1 9.1 Messgrößen (KPIs)

Metrik	Zielwert
Code-Review-Coverage	100%
SAST-Scan-Coverage	100%
Critical/High Findings (Open)	0
Secrets in Code	0

### 37.9.2 9.2 Audit-Nachweise

- Code-Review-Logs
- SAST/DAST-Berichte
- Penetration-Test-Berichte
- Secrets-Rotation-Logs

## 37.10 10. Referenzen

### 37.10.1 Interne Dokumente

- 0380\_Policy\_Secure\_Development.md
- 0340\_Policy\_Vulnerability\_und\_Patch\_Management.md

### **37.10.2 Externe Standards**

- **ISO/IEC 27001:2022 Annex A.8.25** - Secure development lifecycle
  - **ISO/IEC 27001:2022 Annex A.8.26** - Application security requirements
  - **OWASP ASVS** - Application Security Verification Standard
  - **NIST SP 800-218** - Secure Software Development Framework
- 

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 38

## Policy: Incident Management

**Dokument-ID:** 0400

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.24-A.5.28 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 38.1 1. Zweck

Diese Policy definiert die Grundsätze für Incident Management und Security Incident Response der **AdminSend GmbH**. Sie stellt sicher, dass Sicherheitsvorfälle zeitnah erkannt, bewertet, behandelt und dokumentiert werden, um Schäden zu minimieren und aus Vorfällen zu lernen.

### 38.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Incident-Typen:** Security Incidents, Data Breaches, Malware, Phishing, DDoS, Insider Threats
- **Systeme:** Alle IT-Systeme, Anwendungen, Netzwerke, Cloud-Services
- **Personen:** Alle Mitarbeiter, Auftragnehmer, Lieferanten
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_zulässig).

### **38.3 3. Grundsätze (Policy Statements)**

#### **38.3.1 3.1 Incident Response Capability**

Die Organisation unterhält eine Incident Response Capability mit definierten Prozessen, Rollen und Tools zur Behandlung von Sicherheitsvorfällen.

#### **38.3.2 3.2 Meldepflicht**

Alle Mitarbeiter sind verpflichtet, vermutete oder bestätigte Sicherheitsvorfälle unverzüglich zu melden. Es gibt keine negativen Konsequenzen für gutgläubige Meldungen.

#### **38.3.3 3.3 Incident-Kategorisierung und Priorisierung**

Incidents werden nach Schweregrad und Auswirkung kategorisiert: - **Critical:** Schwerwiegende Auswirkungen auf Geschäftsbetrieb oder Datenschutz - **High:** Erhebliche Auswirkungen, aber Geschäftsbetrieb nicht kritisch gefährdet - **Medium:** Moderate Auswirkungen, begrenzte Beeinträchtigung - **Low:** Geringe Auswirkungen, keine unmittelbare Gefahr

#### **38.3.4 3.4 Incident Response Lifecycle**

Incidents werden nach einem strukturierten Prozess behandelt: - **Detection & Reporting:** Erkennung und Meldung - **Triage & Assessment:** Bewertung und Priorisierung - **Containment:** Eindämmung zur Schadensbegrenzung - **Eradication:** Beseitigung der Ursache - **Recovery:** Wiederherstellung des Normalbetriebs - **Post-Incident Review:** Nachbereitung und Lessons Learned

#### **38.3.5 3.5 Eskalation und Kommunikation**

Kritische Incidents werden nach definierten Eskalationspfaden an Management, Legal, PR und ggf. Behörden eskaliert. Kommunikation erfolgt nach festgelegten Kommunikationsplänen.

#### **38.3.6 3.6 Forensik und Evidence Preservation**

Bei schwerwiegenden Incidents wird forensische Analyse durchgeführt. Beweismittel werden sicher gesichert und dokumentiert für mögliche rechtliche Schritte.

#### **38.3.7 3.7 Data Breach Notification**

Data Breaches werden gemäß DSGVO und anderen regulatorischen Anforderungen innerhalb von 72 Stunden an Aufsichtsbehörden und betroffene Personen gemeldet.

#### **38.3.8 3.8 Continuous Improvement**

Aus jedem Incident werden Lessons Learned abgeleitet. Erkenntnisse fließen in die Verbesserung von Prozessen, Kontrollen und Awareness ein.

### **38.4 4. Rollen und Verantwortlichkeiten**

#### **38.4.1 RACI-Matrix: Incident Management**

Aktivität	CISO	Incident Manager	SOC	IT-Betrieb	Legal/DPO	Management
Policy-Erstellung	R/A	C	C	C	C	I
Incident Detection	A	C	R	C	I	I
Incident Triage	A	R	R	C	I	I
Incident Response	A	R	R	R	C	I
Eskalation	A	R	C	I	C	I
Data Breach	A	C	I	I	R	C
Notification						
Forensik	A	C	R	C	C	I
Post-Incident Review	R/A	R	C	C	C	C

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

### 38.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **Incident Manager:** {{ meta.security.incident\_manager }}
- **SOC Manager:** {{ meta.security.soc\_manager }}
- **Data Protection Officer:** {{ meta.dpo.name }}
- **Umsetzungsverantwortliche:** SOC, IT-Betrieb, Incident Response Team
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit

## 38.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

### 38.5.1 Zugehörige Richtlinien

- **0410\_Richtlinie\_Incident\_Response\_und\_Major\_Incident\_Prozess.md** - Detaillierte Implementierungsrichtlinie
- **0320\_PolicyLogging\_und\_Monitoring.md** - Logging and Monitoring Policy
- **0440\_Policy\_Business\_Continuity\_ICT\_Readiness.md** - Business Continuity Policy
- **0560\_Policy\_Datenschutz\_Schnittstellen.md** - Data Protection Policy

### 38.5.2 Zugehörige Standards/Baselinses

- Incident Response Playbooks
- Incident Severity Matrix
- Eskalationspfade

- Data Breach Notification Prozess

### 38.5.3 Zugehörige Prozesse

- Incident Response Prozess
- Major Incident Prozess
- Data Breach Notification Prozess
- Post-Incident Review Prozess

## 38.6 6. Compliance, Monitoring und Durchsetzung

### 38.6.1 Messgrößen und KPIs

- Anzahl Incidents pro Kategorie und Schweregrad
- MTTD (Mean Time To Detect) - Durchschnittliche Erkennungszeit
- MTTR (Mean Time To Respond) - Durchschnittliche Reaktionszeit
- MTTR (Mean Time To Resolve) - Durchschnittliche Lösungszeit
- Anzahl Data Breaches und Meldungen
- Post-Incident Review Completion Rate (Ziel: 100%)

### 38.6.2 Nachweise und Evidence

- Incident-Tickets und Dokumentation
- Incident Response Logs
- Forensik-Reports
- Data Breach Notifications
- Post-Incident Review Reports
- Lessons Learned Dokumentation

### 38.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt: -

**Nicht gemeldeter Incident:** Nachschulung, Verwarnung - **Verzögerte Data Breach Notification:** Compliance-Untersuchung, ggf. Bußgelder - **Beweismittel-Manipulation:** Schwerwiegende

Disziplinarmaßnahmen - **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen

## 38.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet

## 38.8 8. Referenzen

### 38.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0410\_Richtlinie\_Incident\_Response\_und\_Major\_Incident\_Prozess.md - Detailed Guide-line
- 0320\_PolicyLogging\_und\_Monitoring.md - Logging and Monitoring Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

### 38.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.5.24 - Information security incident management planning and preparation
- ISO/IEC 27001:2022 Annex A.5.25 - Assessment and decision on information security events
- ISO/IEC 27001:2022 Annex A.5.26 - Response to information security incidents
- ISO/IEC 27001:2022 Annex A.5.27 - Learning from information security incidents
- ISO/IEC 27001:2022 Annex A.5.28 - Collection of evidence
- NIST SP 800-61 - Computer Security Incident Handling Guide
- DSGVO (EU 2016/679) - Art. 33, 34 - Data Breach Notification
- NIS2-Richtlinie - Network and Information Security Directive

---

#### Genehmigt durch:

{{ meta.management.ceo }}, Geschäftsführung  
Datum: {{ meta.document.approval\_date }}

Nächster Review: {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 39

## Richtlinie: Incident Response und Major Incident Prozess

**Dokument-ID:** 0410

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0400\_Policy\_Incident\_Management.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.24, A.5.25, A.5.26

**Owner:** {{ meta.it\_operations.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Vertraulich

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 39.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0400\_Policy\_Incident\_Management.md und definiert: - Incident-Response-Prozesse und -Workflows - Major-Incident-Management - Security-Incident-Response und Forensik

**Geltungsbereich:** Alle Incidents bei AdminSend GmbH

### 39.2 2. Incident-Kategorien

#### 39.2.1 2.1 Severity-Level

Severity	Definition	Beispiele	Response-Zeit
P1 (Critical)	Kritischer Service-Ausfall	Produktionsausfall, Datenverlust, aktiver Cyberangriff	15 Minuten
P2 (High)	Schwere Beeinträchtigung	Performance-Probleme, Teilausfall	1 Stunde

Severity	Definition	Beispiele	Response-Zeit
P3 (Medium)	Moderate Beeinträchtigung	Einzelne Nutzer betroffen	4 Stunden
	Geringe Beeinträchtigung	Kosmetische Fehler	1 Arbeitstag
P4 (Low)			

### 39.2.2 2.2 Security Incidents

**Kategorien:** - Malware-Infektionen - Phishing-Angriffe - Unauthorized Access - Data Breaches - DDoS-Angriffe - Insider Threats

**Alle Security Incidents mindestens P2**

## 39.3 3. Incident-Response-Prozess

### 39.3.1 3.1 Detection & Reporting

**Meldewege:** - **IT-Support:** {{ meta.support.phone }}, {{ meta.support.email }} - **Security-Team:** {{ meta.security.email }}, {{ meta.security.phone }} - **Self-Service-Portal:** {{ meta.itsm.portal }}

**Pflichtangaben:** - Beschreibung des Problems - Betroffene Systeme/Nutzer - Zeitpunkt des Auftretens - Auswirkungen

### 39.3.2 3.2 Triage & Classification

**Prozess:** 1. Incident-Ticket erstellen 2. Severity-Level bestimmen 3. Kategorie zuordnen 4. Zuständiges Team zuweisen 5. Erste Response innerhalb SLA

**Eskalation:** - P1: Sofortige Eskalation an On-Call - P2: Eskalation nach 1 Stunde ohne Fortschritt - Security Incidents: Parallel an Security-Team

### 39.3.3 3.3 Investigation & Diagnosis

**Schritte:** 1. Symptome analysieren 2. Logs prüfen 3. Betroffene Systeme identifizieren 4. Root Cause ermitteln 5. Workaround identifizieren (falls möglich)

**Dokumentation:** - Alle Schritte im Ticket dokumentieren - Logs und Screenshots anhängen - Zeitstempel für alle Aktionen

### 39.3.4 3.4 Resolution & Recovery

**Prozess:** 1. Fix implementieren oder Workaround anwenden 2. Funktionstest durchführen 3. Nutzer informieren 4. Monitoring auf Wiederauftreten

**Verifizierung:** - Nutzer bestätigt Lösung - Monitoring zeigt normale Werte - Keine weiteren Meldungen

### **39.3.5 3.5 Closure & Post-Incident Review**

**Closure:** - Ticket schließen nach Nutzer-Bestätigung - Dokumentation vervollständigen - Kategorisierung prüfen

**Post-Incident Review (PIR):** - Bei P1/P2 Incidents verpflichtend - Innerhalb 7 Tage nach Closure - Lessons Learned dokumentieren - Verbesserungsmaßnahmen definieren

## **39.4 4. Major Incident Management**

### **39.4.1 4.1 Major Incident Kriterien**

**Ein Incident ist "Major" wenn:** - Severity P1 - Mehrere kritische Services betroffen - Viele Nutzer betroffen (> 100) - Medienaufmerksamkeit möglich - Regulatorische Meldepflicht

### **39.4.2 4.2 Major Incident Team**

**Rollen:** - **Incident Manager:** Koordination, Kommunikation - **Technical Lead:** Technische Lösung - **Communications Lead:** Stakeholder-Kommunikation - **Security Lead:** Bei Security Incidents - **Management Representative:** Entscheidungen

**Verfügbarkeit:** 24/7 On-Call-Rotation

### **39.4.3 4.3 Major Incident Prozess**

**Phase 1: Mobilisierung (0-15 Minuten)** 1. Major Incident deklarieren 2. Major Incident Team alarmieren 3. War Room einrichten (physisch oder virtuell) 4. Incident-Bridge aufbauen (Telefonkonferenz)

**Phase 2: Containment (15-60 Minuten)** 1. Auswirkungen begrenzen 2. Workaround implementieren (falls möglich) 3. Stakeholder informieren 4. Monitoring intensivieren

**Phase 3: Resolution (variabel)** 1. Root Cause identifizieren 2. Permanente Lösung implementieren 3. Schrittweise Wiederherstellung 4. Verifizierung

**Phase 4: Recovery (variabel)** 1. Alle Services wiederhergestellt 2. Monitoring auf Normalzustand 3. Nutzer informieren 4. Major Incident beenden

**Phase 5: Post-Incident Review (innerhalb 48 Stunden)** 1. Timeline rekonstruieren 2. Root Cause Analysis 3. Lessons Learned 4. Action Items definieren 5. Management-Bericht

### **39.4.4 4.4 Kommunikation**

**Interne Kommunikation:** - Status-Updates alle 30 Minuten - Stakeholder-Benachrichtigungen - Intranet-Status-Page

**Externe Kommunikation:** - Kunden-Benachrichtigungen (falls zutreffend) - Medien-Statement (bei Bedarf) - Regulatorische Meldungen

## 39.5 5. Security Incident Response

### 39.5.1 5.1 Security Incident Response Team (SIRT)

**Mitglieder:** - CISO oder Security Lead - IT-Security-Analysten - IT-Forensik-Experte - Legal/Compliance - HR (bei Insider Threats)

### 39.5.2 5.2 Security Incident Prozess

**Phase 1: Preparation** - Incident-Response-Plan aktuell - Tools und Playbooks bereit - Team geschult

**Phase 2: Identification** - Security-Event detektiert (SIEM, EDR, etc.) - Triage: Ist es ein Incident? - Severity bestimmen

**Phase 3: Containment** - **Short-term:** Sofortige Maßnahmen (Account sperren, Netzwerk isolieren) - **Long-term:** Dauerhafte Isolation

**Phase 4: Eradication** - Malware entfernen - Schwachstellen patchen - Kompromittierte Credentials ändern

**Phase 5: Recovery** - Systeme wiederherstellen - Monitoring intensivieren - Schrittweise Rückkehr zum Normalbetrieb

**Phase 6: Lessons Learned** - Post-Incident Review - Playbook-Updates - Training-Bedarf identifizieren

### 39.5.3 5.3 Forensik

**Wann erforderlich:** - Data Breaches - Insider Threats - Rechtliche Ermittlungen - Schwere Security Incidents

**Prozess:** 1. **Preservation:** Beweise sichern 2. **Collection:** Daten sammeln (Disk Images, Logs, Memory Dumps) 3. **Analysis:** Forensische Analyse 4. **Reporting:** Forensik-Bericht 5. **Chain of Custody:** Lückenlose Dokumentation

**Tools:** {{ meta.security.forensics\_tools }}

### 39.5.4 5.4 Meldepflichten

**Intern:** - CISO: Sofort - Management: Innerhalb 4 Stunden - Datenschutzbeauftragter: Bei Datenschutzverletzung

**Extern:** - **DSGVO:** Datenschutzbehörde innerhalb 72 Stunden (bei Datenschutzverletzung) - **Betroffene Personen:** Ohne unangemessene Verzögerung - **Strafverfolgung:** Bei kriminellen Handlungen

## 39.6 6. Incident-Kommunikation

### 39.6.1 6.1 Status-Updates

**Frequenz:** - P1: Alle 30 Minuten - P2: Alle 2 Stunden - P3/P4: Täglich

**Kanäle:** - E-Mail an Stakeholder - Status-Page ({{ meta.status.url }}) - Intranet-Benachrichtigungen

## 39.6.2 6.2 Stakeholder-Matrix

Stakeholder	P1	P2	P3	P4
Betroffene Nutzer	Sofort	1h	4h	1d
Management	15min	2h	-	-
CISO (Security)	Sofort	Sofort	4h	-
Kunden (extern)	1h	4h	-	-

## 39.7 7. Compliance und Audit

### 39.7.1 7.1 Messgrößen (KPIs)

Metrik	Zielwert
P1 Response-Zeit	< 15 Minuten
P1 Resolution-Zeit	< 4 Stunden
Major Incident PIR-Completion	100%
Security Incident Detection-Zeit	< 1 Stunde

### 39.7.2 7.2 Audit-Nachweise

- Incident-Tickets und -Logs
- Post-Incident-Review-Berichte
- Kommunikations-Logs
- Forensik-Berichte (bei Security Incidents)

## 39.8 8. Referenzen

### 39.8.1 Interne Dokumente

- 0400\_Policy\_Incident\_Management.md
- 0320\_PolicyLogging\_und\_Monitoring.md

### 39.8.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.5.24 - Information security incident management planning
- ISO/IEC 27001:2022 Annex A.5.25 - Assessment and decision on information security events
- ISO/IEC 27001:2022 Annex A.5.26 - Response to information security incidents
- NIST SP 800-61 - Computer Security Incident Handling Guide

---

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 40

## Policy: Backup und Wiederherstellung

**Dokument-ID:** 0420

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.8.13 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 40.1 1. Zweck

Diese Policy definiert die Grundsätze für Backup und Wiederherstellung der **AdminSend GmbH**. Sie stellt sicher, dass kritische Daten und Systeme im Falle von Datenverlust, Korruption oder Katastrophen wiederhergestellt werden können.

### 40.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Systeme:** Alle IT-Systeme, Datenbanken, Anwendungen, Dateisysteme, VMs, Cloud-Ressourcen
- **Daten:** Alle geschäftskritischen und personenbezogenen Daten
- **Backup-Typen:** Full, Incremental, Differential, Snapshot, Cloud Backup
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_) zulässig.

## 40.3 3. Grundsätze (Policy Statements)

### 40.3.1 3.1 Backup-Strategie basierend auf RPO/RTO

Backup-Strategien werden basierend auf Recovery Point Objective (RPO) und Recovery Time Objective (RTO) definiert: - **Kritische Systeme:** RPO < 1 Stunde, RTO < 4 Stunden - **Wichtige Systeme:** RPO < 24 Stunden, RTO < 24 Stunden - **Standard-Systeme:** RPO < 7 Tage, RTO < 72 Stunden

### 40.3.2 3.2 3-2-1 Backup-Regel

Backups folgen der 3-2-1-Regel: - **3** Kopien der Daten (Original + 2 Backups) - **2** verschiedene Speichermedien/Technologien - **1** Kopie offline (Air-Gapped oder geografisch getrennt)

### 40.3.3 3.3 Verschlüsselte Backups

Alle Backups werden verschlüsselt gespeichert (at rest) und übertragen (in transit). Verschlüsselungsschlüssel werden sicher verwaltet und getrennt von Backups gespeichert.

### 40.3.4 3.4 Regelmäßige Backup-Tests

Backups werden regelmäßig getestet, um die Wiederherstellbarkeit sicherzustellen: - **Kritische Systeme:** Monatliche Restore-Tests - **Wichtige Systeme:** Quartalsweise Restore-Tests - **Standard-Systeme:** Jährliche Restore-Tests

### 40.3.5 3.5 Immutable Backups

Kritische Backups werden als immutable (unveränderlich) gespeichert, um Schutz vor Ransomware und versehentlicher Löschung zu bieten.

### 40.3.6 3.6 Backup-Monitoring und Alerting

Backup-Jobs werden kontinuierlich überwacht. Fehlgeschlagene Backups lösen sofortige Alerts aus und werden priorisiert behoben.

### 40.3.7 3.7 Retention und Aufbewahrung

Backups werden entsprechend gesetzlicher, regulatorischer und geschäftlicher Anforderungen aufbewahrt: - **Tägliche Backups:** 30 Tage - **Wöchentliche Backups:** 12 Wochen - **Monatliche Backups:** 12 Monate - **Jährliche Backups:** 7 Jahre (oder nach Compliance-Anforderungen)

### 40.3.8 3.8 Disaster Recovery Integration

Backup-Strategien sind in die Disaster Recovery und Business Continuity Pläne integriert.

## 40.4 4. Rollen und Verantwortlichkeiten

### 40.4.1 RACI-Matrix: Backup und Wiederherstellung

Aktivität	CISO	Backup Administrator	IT-Betrieb	System Owner	BCM Manager
Policy-Erstellung	R/A	C	C	C	C
Backup-Konfiguration	C	R/A	C	C	I
Backup-Durchführung	I	R/A	C	I	I
Backup-Monitoring	C	R/A	C	I	I
Restore-Tests	C	R	R	R/A	C
Disaster Recovery	A	C	R	C	R
Compliance-Prüfung	R/A	C	I	I	C

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

#### 40.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **Backup Administrator:** {{ meta.it.backup\_admin }}
- **BCM Manager:** {{ meta.bcm.manager }}
- **Umsetzungsverantwortliche:** IT-Betrieb, System Owner
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit

### 40.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

#### 40.5.1 Zugehörige Richtlinien

- **0430\_Richtlinie\_Backup\_Restore\_und\_Regelmaessige\_Tests.md** - Detaillierte Implementierungsrichtlinie
- **0440\_Policy\_Business\_Continuity\_ICT\_Readiness.md** - Business Continuity Policy
- **0260\_Policy\_Kryptografie\_und\_Schluesselmanagement.md** - Cryptography Policy
- **0580\_Policy\_Aufbewahrung\_und\_Loeschung.md** - Retention Policy

#### 40.5.2 Zugehörige Standards/Baselinses

- RPO/RTO-Matrix
- Backup-Schedule
- Retention-Anforderungen
- Restore-Test-Prozeduren

### 40.5.3 Zugehörige Prozesse

- Backup-Prozess
- Restore-Prozess
- Backup-Test-Prozess
- Disaster Recovery Prozess

## 40.6 6. Compliance, Monitoring und Durchsetzung

### 40.6.1 Messgrößen und KPIs

- Backup Success Rate (Ziel: 99.9%)
- Anzahl fehlgeschlagener Backups
- Durchschnittliche Backup-Dauer
- Restore Success Rate (Ziel: 100%)
- Durchschnittliche Restore-Dauer (RTO-Compliance)
- Backup-Test-Completion-Rate (Ziel: 100%)

### 40.6.2 Nachweise und Evidence

- Backup-Logs und Job-Status
- Restore-Test-Protokolle
- Backup-Monitoring-Reports
- Disaster Recovery Test Reports
- Compliance-Nachweise (Retention)
- Audit-Berichte zu Backup-Compliance

### 40.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:

- **Fehlende Backups:** Sofortige Remediation, Untersuchung - **Nicht getestete Backups:** Nachholung, Nachschulung - **Unverschlüsselte Backups:** Sofortige Verschlüsselung, Untersuchung - **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen

## 40.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und System Owner genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet
- **Kompensationsmaßnahmen:** Ausnahmen erfordern alternative Sicherheitsmaßnahmen

## 40.8 8. Referenzen

### 40.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy

- 0430\_Richtlinie\_Backup\_Restore\_und\_Regelmaessige\_Tests.md - Detailed Guideline
- 0440\_Policy\_Business\_Continuity ICT\_ Readiness.md - Business Continuity Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

#### 40.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.8.13 - Information backup
  - ISO/IEC 27002:2022 - Information security controls
  - ISO 22301 - Business Continuity Management
  - DSGVO (EU 2016/679) - Datenschutz-Grundverordnung (Backup von personenbezogenen Daten)
- 

**Genehmigt durch:**

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 41

## Richtlinie: Backup, Restore und Regelmäßige Tests

**Dokument-ID:** 0430

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0420\_Policy\_Backup\_und\_Wiederherstellung.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.8.13

**Owner:** {{ meta.it\_operations.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Vertraulich

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 41.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0420\_Policy\_Backup\_und\_Wiederherstellung.md und definiert:  
- Backup-Strategien und -Frequenzen - Restore-Prozesse und -Tests - Backup-Monitoring und -Verifizierung

**Geltungsbereich:** Alle Daten und Systeme bei **AdminSend GmbH**

### 41.2 2. Backup-Strategie

#### 41.2.1 2.1 3-2-1-Regel

**Prinzip:** - **3** Kopien der Daten (1 Produktion + 2 Backups) - **2** verschiedene Medientypen (z.B. Disk + Tape/Cloud) - **1** Kopie Off-Site (geografisch getrennt)

#### 41.2.2 2.2 Backup-Typen

**Full Backup:** - Vollständige Sicherung aller Daten - Frequenz: Wöchentlich (Sonntag) - Längste Restore-Zeit, aber einfachste Wiederherstellung

**Incremental Backup:** - Nur Änderungen seit letztem Backup - Frequenz: Täglich - Schnellstes Backup, längere Restore-Zeit

**Differential Backup:** - Änderungen seit letztem Full Backup - Frequenz: Optional, bei Bedarf - Balance zwischen Full und Incremental

### 41.2.3 2.3 Backup-Frequenzen

System-Typ	Full	Incremental	RPO	RTO
Kritische Datenbanken	Täglich	Stündlich	1h	4h
Produktionsserver	Wöchentlich	Täglich	24h	8h
Fileserver	Wöchentlich	Täglich	24h	8h
Workstations	Monatlich	Wöchentlich	7d	24h
E-Mail	Täglich	Stündlich	1h	4h

**RPO (Recovery Point Objective):** Maximaler Datenverlust

**RTO (Recovery Time Objective):** Maximale Wiederherstellungszeit

## 41.3 3. Backup-Implementierung

### 41.3.1 3.1 Backup-Systeme

**On-Premises:** - **Backup-Server:** {{ meta.backup.server }} - **Backup-Software:** {{ meta.backup.software }} (z.B. Veeam, Commvault) - **Storage:** {{ meta.backup.storage }} (Disk, Tape)

**Cloud-Backup:** - **Cloud-Provider:** {{ meta.cloud.backup\_provider }} (z.B. Azure Backup, AWS Backup) - **Verschlüsselung:** AES-256 - **Geo-Redundanz:** Aktiviert

### 41.3.2 3.2 Backup-Zeitfenster

**Produktionssysteme:** - Backup-Window: 22:00 - 06:00 Uhr - Minimale Performance-Beeinträchtigung - Monitoring während Backup

**Entwicklungssysteme:** - Backup-Window: Jederzeit - Keine Performance-Anforderungen

### 41.3.3 3.3 Verschlüsselung

**In Transit:** - TLS 1.2+ für Backup-Übertragung - VPN für Off-Site-Backups

**At Rest:** - AES-256 Verschlüsselung aller Backups - Schlüsselverwaltung über Key Vault - Separate Schlüssel für Backups

### 41.3.4 3.4 Retention

**Retention-Schema (GFS - Grandfather-Father-Son):** - **Daily:** 7 Tage - **Weekly:** 4 Wochen - **Monthly:** 12 Monate - **Yearly:** {{ meta.retention.backup\_years }} Jahre

**Compliance-Backups:** - Finanzdaten: 10 Jahre - Personaldaten: Gemäß DSGVO - E-Mails: {{ meta.retention.email\_years }} Jahre

## 41.4 4. Restore-Prozesse

### 41.4.1 4.1 Restore-Typen

**File-Level Restore:** - Einzelne Dateien oder Ordner - Self-Service für Nutzer (begrenzt) - IT-Support für umfangreichere Restores

**System-Level Restore:** - Vollständige Server-Wiederherstellung - Bare-Metal-Recovery - Nur durch IT-Betrieb

**Database Restore:** - Point-in-Time-Recovery - Transaktions-Logs - Nur durch Database-Admins

### 41.4.2 4.2 Restore-Prozess

**Schritt 1: Anforderung** - Ticket erstellen mit Details (Was, Wann, Warum) - Genehmigung durch Vorgesetzten (bei umfangreichen Restores)

**Schritt 2: Vorbereitung** - Backup-Katalog prüfen - Restore-Ziel vorbereiten - Downtime planen (falls erforderlich)

**Schritt 3: Restore** - Restore durchführen - Fortschritt überwachen - Fehlerbehandlung

**Schritt 4: Verifizierung** - Datenintegrität prüfen - Funktionstest - Nutzer-Bestätigung

**Schritt 5: Dokumentation** - Restore-Log - Lessons Learned - Ticket schließen

### 41.4.3 4.3 Disaster Recovery

**Bei Totalausfall:** 1. Disaster Recovery Plan aktivieren 2. Alternative Infrastruktur bereitstellen 3. Kritische Systeme zuerst wiederherstellen 4. Schrittweise Wiederherstellung weiterer Systeme 5. Verifizierung und Rückkehr zum Normalbetrieb

**Details:** Siehe 0160\_Disaster\_Recovery\_und\_Business\_Continuity.md (IT-Operation Templates)

## 41.5 5. Backup-Monitoring

### 41.5.1 5.1 Überwachte Metriken

**Backup-Jobs:** - Erfolgreiche/Fehlgeschlagene Backups - Backup-Dauer - Backup-Größe - Änderungsrate

**Storage:** - Verfügbarer Speicherplatz - Wachstumsrate - Deduplizierungsrate

**Performance:** - Backup-Geschwindigkeit - Netzwerk-Auslastung - Storage-Performance

### 41.5.2 5.2 Alerting

**Kritische Alerts:** - Backup fehlgeschlagen (2x hintereinander) - Storage > 90% voll - Backup-Window überschritten - Verschlüsselung fehlgeschlagen

**Eskalation:** - Erste Benachrichtigung: Backup-Admin - Nach 2 Stunden: IT-Operations-Manager - Nach 4 Stunden: CISO (bei kritischen Systemen)

### 41.5.3 5.3 Reporting

**Täglicher Backup-Report:** - Status aller Backup-Jobs - Fehlgeschlagene Backups - Storage-Auslastung

**Monatlicher Management-Report:** - Backup-Success-Rate - Restore-Statistiken - Kapazitätsplanung - Compliance-Status

## 41.6 6. Backup-Tests

### 41.6.1 6.1 Test-Frequenzen

Test-Typ	Frequenz	Durchführung
File-Level Restore	Monatlich	Stichprobe
System-Level Restore	Quartalsweise	Kritische Systeme
Database Restore	Monatlich	Point-in-Time-Recovery
Disaster Recovery	Jährlich	Vollständiger DR-Test

### 41.6.2 6.2 Test-Prozess

**Planung:** 1. Test-Scope definieren 2. Test-Zeitfenster festlegen 3. Stakeholder informieren 4. Test-Umgebung vorbereiten

**Durchführung:** 1. Restore in Test-Umgebung 2. Datenintegrität prüfen 3. Funktionstest 4. Performance-Test 5. Zeitnahme (RTO-Verifizierung)

**Dokumentation:** 1. Test-Protokoll erstellen 2. Erfolg/Misserfolg dokumentieren 3. Probleme und Lessons Learned 4. Verbesserungsmaßnahmen definieren

**Nachbereitung:** 1. Test-Umgebung bereinigen 2. Backup-Prozesse anpassen (falls erforderlich) 3. Management-Bericht

### 41.6.3 6.3 Disaster Recovery Drill

**Jährlicher DR-Test:** - Simulation eines Totalausfalls - Aktivierung des DR-Plans - Wiederherstellung kritischer Systeme - Zeitnahme und Dokumentation - Management-Präsentation

**Teilnehmer:** - IT-Betrieb - Application-Owner - Management - Business-Vertreter

## 41.7 7. Backup-Sicherheit

### 41.7.1 7.1 Zugriffskontrolle

**Berechtigungen:** - **Backup-Admins:** Vollzugriff auf Backup-System - **System-Admins:** Restore-Berechtigung für eigene Systeme - **Nutzer:** Self-Service-Restore (begrenzt)

**Authentifizierung:** - MFA für Backup-System-Zugriff - Privilegierte Accounts für Backup-Admins

## 41.7.2 7.2 Immutable Backups

**Schutz vor Ransomware:** - Immutable Backups (Write-Once-Read-Many) - Air-Gapped Backups (offline) - Separate Credentials für Backup-Storage

**Retention Lock:** - Backups können nicht vorzeitig gelöscht werden - Schutz vor versehentlicher oder böswilliger Löschung

## 41.7.3 7.3 Audit-Logging

**Protokollierte Events:** - Backup-Job-Starts und -Ends - Restore-Anforderungen und -Durchführungen - Konfigurationsänderungen - Zugriffe auf Backup-System

**Retention:** {{ meta.retention.log\_years }} Jahre

# 41.8 8. Compliance und Audit

## 41.8.1 8.1 Messgrößen (KPIs)

Metrik	Zielwert
Backup-Success-Rate	> 99%
Restore-Success-Rate	100%
RTO-Einhaltung	100%
RPO-Einhaltung	100%
Test-Completion-Rate	100%

## 41.8.2 8.2 Audit-Nachweise

- Backup-Logs und -Reports
- Restore-Test-Protokolle
- DR-Drill-Dokumentation
- Compliance-Berichte

# 41.9 9. Referenzen

## 41.9.1 Interne Dokumente

- 0420\_Policy\_Backup\_und\_Wiederherstellung.md
- 0160\_Disaster\_Recovery\_und\_Business\_Continuity.md (IT-Operation)

## 41.9.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.8.13 - Information backup
- NIST SP 800-34 - Contingency Planning Guide

---

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 42

## Policy: Business Continuity ICT Readiness

**Dokument-ID:** 0440

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.29, A.5.30 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 42.1 1. Zweck

Diese Policy definiert die Grundsätze für ICT Continuity und Disaster Recovery der **AdminSend GmbH**. Sie stellt sicher, dass IT-Systeme und -Services während Störungen weiterbetrieben oder schnell wiederhergestellt werden können, um die Geschäftskontinuität zu gewährleisten.

### 42.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Systeme:** Alle geschäftskritischen IT-Systeme, Anwendungen, Infrastruktur, Cloud-Services
- **Szenarien:** Naturkatastrophen, Cyberangriffe, Systemausfälle, Pandemien, Lieferantenausfälle
- **Schnittstellen:** Integration mit BCM (Business Continuity Management)
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_) zulässig.

## **42.3 3. Grundsätze (Policy Statements)**

### **42.3.1 3.1 ICT Continuity Planning**

Für alle geschäftskritischen IT-Services existieren ICT Continuity Pläne, die Wiederherstellungsstrategien, Ressourcen und Verantwortlichkeiten definieren.

### **42.3.2 3.2 Business Impact Analysis (BIA)**

Regelmäßige Business Impact Analysen identifizieren kritische IT-Services und deren RPO/RTO-Anforderungen. Die BIA wird mit dem BCM-Team koordiniert.

### **42.3.3 3.3 Redundanz und Hochverfügbarkeit**

Kritische IT-Systeme werden mit Redundanz und Hochverfügbarkeit ausgelegt: - Redundante Komponenten (Server, Storage, Netzwerk) - Geografisch verteilte Rechenzentren - Load Balancing und Failover-Mechanismen - Cloud-basierte Disaster Recovery

### **42.3.4 3.4 Disaster Recovery Pläne (DRP)**

Detaillierte Disaster Recovery Pläne beschreiben Schritt-für-Schritt-Prozeduren zur Wiederherstellung von IT-Systemen nach einem Ausfall.

### **42.3.5 3.5 Regelmäßige Tests und Übungen**

ICT Continuity und DR-Pläne werden regelmäßig getestet: - **Kritische Systeme:** Jährliche DR-Tests - **Wichtige Systeme:** Alle 2 Jahre - **Tabletop-Übungen:** Quartalsweise

### **42.3.6 3.6 Alternative Arbeitsplätze und Remote Work**

Mitarbeiter können bei Standortausfällen von alternativen Standorten oder remote arbeiten. Remote-Access-Infrastruktur ist hochverfügbar ausgelegt.

### **42.3.7 3.7 Lieferanten- und Cloud-Provider-Continuity**

Kritische Lieferanten und Cloud-Provider werden auf ihre Business Continuity Fähigkeiten geprüft. SLAs enthalten Continuity-Anforderungen.

### **42.3.8 3.8 Incident-to-Crisis-Eskalation**

Klare Eskalationspfade definieren, wann ein IT-Incident zu einer Business Continuity Crisis eskaliert wird und das BCM-Team aktiviert wird.

## **42.4 4. Rollen und Verantwortlichkeiten**

### **42.4.1 RACI-Matrix: Business Continuity ICT Readiness**

Aktivität	CISO	BCM Manager	IT-Betrieb	CIO	Crisis Management Team
Policy-Erstellung	R/A	C	C	C	I
BIA-Durchführung	C	R/A	C	C	I
DRP-Erstellung	A	C	R	C	I
DR-Tests	A	C	R	C	I
Crisis Activation	C	R/A	C	C	R
Recovery Execution	A	C	R	R	C
Post-Incident Review	R/A	R	C	C	C

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

#### 42.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **BCM Manager:** {{ meta.bcm.manager }}
- **DR Coordinator:** {{ meta.it.drCoordinator }}
- **CIO:** Anna Schmidt
- **Umsetzungsverantwortliche:** IT-Betrieb, System Owner
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit

### 42.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

#### 42.5.1 Zugehörige Richtlinien

- **0450\_Richtlinie\_ICT\_DR\_Schnittstellen\_zu\_BCM.md** - Detaillierte Implementierungsrichtlinie
- **0420\_Policy\_Backup\_und\_Wiederherstellung.md** - Backup Policy
- **0400\_Policy\_Incident\_Management.md** - Incident Management Policy
- BCM-Handbuch (siehe templates/de/bcm/)

#### 42.5.2 Zugehörige Standards/Baselinses

- RPO/RTO-Matrix
- DR-Plan-Templates
- Test-Szenarien
- Eskalationspfade

### 42.5.3 Zugehörige Prozesse

- Business Impact Analysis Prozess
- Disaster Recovery Prozess
- DR-Test-Prozess
- Crisis Management Prozess

## 42.6 6. Compliance, Monitoring und Durchsetzung

### 42.6.1 Messgrößen und KPIs

- Anzahl kritischer Systeme mit DR-Plänen (Ziel: 100%)
- DR-Test-Completion-Rate (Ziel: 100%)
- Durchschnittliche Recovery Time (RTO-Compliance)
- Anzahl erfolgreicher DR-Tests
- BIA-Aktualität (Ziel: jährliche Aktualisierung)
- Verfügbarkeit kritischer Systeme (Ziel: 99.9%)

### 42.6.2 Nachweise und Evidence

- Business Impact Analysis Reports
- Disaster Recovery Pläne
- DR-Test-Protokolle
- Verfügbarkeits-Metriken
- Crisis Management Übungsprotokolle
- Audit-Berichte zu BCM/DR

### 42.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:

- **Fehlende DR-Pläne:** Sofortige Erstellung, Eskalation
- **Nicht getestete DR-Pläne:** Nachholung, Nachschulung
- **RTO/RPO-Verletzungen:** Root Cause Analysis, Remediation
- **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen

## 42.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und BCM Manager genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet
- **Kompensationsmaßnahmen:** Ausnahmen erfordern alternative Continuity-Maßnahmen

## 42.8 8. Referenzen

### 42.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy

- 0450\_Richtlinie\_ICT\_DR\_Schnittstellen\_zu\_BCM.md - Detailed Guideline
- 0420\_Policy\_Backup\_und\_Wiederherstellung.md - Backup Policy
- BCM-Handbuch (templates/de/bcm/)

#### 42.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.5.29 - Information security during disruption
  - ISO/IEC 27001:2022 Annex A.5.30 - ICT readiness for business continuity
  - ISO 22301 - Business Continuity Management Systems
  - ISO/IEC 27031 - ICT readiness for business continuity
  - BSI Standard 100-4 - Business Continuity Management
- 

**Genehmigt durch:**

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 43

## Richtlinie: ICT Disaster Recovery - Schnittstellen zu BCM

**Dokument-ID:** 0450

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0440\_Policy\_Business\_Continuity\_ICT\_Readiness.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.29, A.5.30

**Owner:** {{ meta.it\_operations.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Vertraulich

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 43.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0440\_Policy\_Business\_Continuity\_ICT\_Readiness.md und definiert:  
- ICT Disaster Recovery Pläne und Prozesse  
- Schnittstellen zum Business Continuity Management (BCM)  
- ICT-Readiness für Notfallsituationen

**Geltungsbereich:** Alle IT-Systeme und -Services bei AdminSend GmbH

### 43.2 2. ICT Disaster Recovery Strategie

#### 43.2.1 2.1 Recovery-Ziele

**RTO (Recovery Time Objective):** | System-Tier | RTO | Begründung | |—————|——|——|——|  
| Tier 1 (Kritisch) | 4 Stunden | Geschäftskritische Systeme | | Tier 2 (Wichtig) | 24 Stunden |  
Wichtige Business-Funktionen | | Tier 3 (Standard) | 72 Stunden | Standard-IT-Services |

**RPO (Recovery Point Objective):** | System-Tier | RPO | Backup-Frequenz | |—————|——|——|——|  
| Tier 1 | 1 Stunde | Stündlich | | Tier 2 | 24 Stunden | Täglich | | Tier 3 | 7 Tage |  
Wöchentlich |

### 43.2.2 2.2 DR-Strategien

**Hot Site:** - Vollständig redundante Infrastruktur - Echtzeit-Replikation - Sofortige Failover-Fähigkeit - Für Tier 1 Systeme

**Warm Site:** - Teilweise vorkonfigurierte Infrastruktur - Regelmäßige Backups - Aktivierung innerhalb Stunden - Für Tier 2 Systeme

**Cold Site:** - Grundinfrastruktur vorhanden - Wiederherstellung aus Backups - Aktivierung innerhalb Tagen - Für Tier 3 Systeme

## 43.3 3. DR-Infrastruktur

### 43.3.1 3.1 Primäres Rechenzentrum

**Standort:** {{ netbox.site.primary }}

**Systeme:** Alle Produktionssysteme

**Redundanz:** N+1 für kritische Komponenten

### 43.3.2 3.2 DR-Standort

**Standort:** {{ netbox.site.dr }}

**Entfernung:** > 50 km vom Primärstandort

**Systeme:** Replizierte Tier 1 Systeme, Backup-Infrastruktur

### 43.3.3 3.3 Cloud-DR

**Cloud-Provider:** {{ meta.cloud.dr\_provider }}

**Regionen:** {{ meta.cloud.primary\_region }}, {{ meta.cloud.dr\_region }}

**Services:** IaaS für DR-Workloads

## 43.4 4. Schnittstellen zu BCM

### 43.4.1 4.1 Business Impact Analysis (BIA)

**ICT-Input für BIA:** - System-Abhängigkeiten - RTO/RPO-Fähigkeiten - Single Points of Failure - Wiederherstellungskosten

**BIA-Output für ICT:** - Kritikalität der Business-Prozesse - Maximale Ausfalltoleranz (MTD) - Priorisierung der Wiederherstellung

### 43.4.2 4.2 BCM-Pläne

**ICT-Beiträge:** - IT Disaster Recovery Plan (DRP) - Technische Wiederherstellungsprozeduren - Kontaktlisten IT-Personal - Eskalationspfade

**BCM-Koordination:** - Abstimmung mit Business Continuity Plans (BCP) - Gemeinsame Übungen und Tests - Konsistente Kommunikation

### **43.4.3 4.3 Krisenmanagement**

**ICT-Rolle im Krisenstab:** - IT-Vertreter im Krisenstab - Status-Updates zu IT-Systemen - Technische Entscheidungsunterstützung - Koordination der IT-Wiederherstellung

## **43.5 5. DR-Aktivierung**

### **43.5.1 5.1 Aktivierungskriterien**

**Automatische Aktivierung:** - Kompletter Ausfall Primärstandort - Kritische Infrastrukturkomponenten ausgefallen - Naturkatastrophen

**Manuelle Aktivierung:** - Entscheidung durch Krisenstab - Geplante Failover-Tests - Wartungsarbeiten

### **43.5.2 5.2 Aktivierungsprozess**

**Phase 1: Assessment (0-30 Minuten)** 1. Schadensumfang bewerten 2. DR-Aktivierung entscheiden 3. Krisenstab informieren 4. DR-Team mobilisieren

**Phase 2: Activation (30 Minuten - 4 Stunden)** 1. DR-Infrastruktur aktivieren 2. Systeme wiederherstellen (nach Priorität) 3. Netzwerk-Routing umstellen 4. Funktionstest

**Phase 3: Operation (variabel)** 1. Betrieb im DR-Modus 2. Monitoring intensivieren 3. Regelmäßige Status-Updates 4. Vorbereitung Rückkehr

**Phase 4: Fallback (geplant)** 1. Primärstandort wiederherstellen 2. Daten synchronisieren 3. Geplanter Fallback 4. Verifizierung

## **43.6 6. DR-Tests**

### **43.6.1 6.1 Test-Typen**

**Tabletop-Exercise:** - Frequenz: Quartalsweise - Durchsprache des DR-Plans - Keine technische Aktivierung

**Partial Failover:** - Frequenz: Halbjährlich - Einzelne Systeme failover - Minimale Business-Auswirkung

**Full DR-Drill:** - Frequenz: Jährlich - Kompletter Failover aller Tier 1 Systeme - Geplante Downtime erforderlich

### **43.6.2 6.2 Test-Dokumentation**

**Test-Protokoll:** - Datum, Teilnehmer, Scope - Durchgeführte Schritte - Gemessene RTO/RPO - Probleme und Lessons Learned - Verbesserungsmaßnahmen

## **43.7 7. Compliance und Audit**

### **43.7.1 7.1 Messgrößen (KPIs)**

Metrik	Zielwert
DR-Test-Success-Rate	100%
RTO-Einhaltung (Test)	100%
RPO-Einhaltung (Test)	100%
DR-Plan-Aktualität	< 6 Monate

### 43.7.2 7.2 Audit-Nachweise

- DR-Pläne und -Prozeduren
- Test-Protokolle
- BIA-Dokumentation
- Failover-Logs

## 43.8 8. Referenzen

### 43.8.1 Interne Dokumente

- 0440\_Policy\_Business\_Continuity\_ICT\_Readiness.md
- 0430\_Richtlinie\_Backup\_Restore\_und\_Regelmaessige\_Tests.md
- BCM-Handbuch (falls vorhanden)

### 43.8.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.5.29 - Information security during disruption
- ISO/IEC 27001:2022 Annex A.5.30 - ICT readiness for business continuity
- ISO 22301 - Business Continuity Management

---

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

## Chapter 44

# Policy: Lieferanten und Cloud Sicherheit

**Dokument-ID:** 0460

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.19-A.5.23 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 44.1 1. Zweck

Diese Policy definiert die Grundsätze für Lieferanten- und Cloud-Sicherheitsmanagement der **AdminSend GmbH**. Sie stellt sicher, dass Lieferanten, Dienstleister und Cloud-Provider Sicherheitsanforderungen erfüllen und über ihren gesamten Lebenszyklus sicher verwaltet werden.

### 44.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Lieferanten-Typen:** IT-Dienstleister, Cloud-Provider, SaaS-Anbieter, Outsourcing-Partner, Subunternehmer
- **Services:** IaaS, PaaS, SaaS, Managed Services, Outsourcing
- **Lebenszyklus:** Auswahl, Onboarding, Betrieb, Monitoring, Offboarding
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_) zulässig.

## **44.3 3. Grundsätze (Policy Statements)**

### **44.3.1 3.1 Third-Party Risk Assessment**

Alle Lieferanten werden vor Vertragsabschluss einem Sicherheits-Risk-Assessment unterzogen. Das Assessment berücksichtigt Datenzugriff, Kritikalität und Compliance-Anforderungen.

### **44.3.2 3.2 Vertragliche Sicherheitsanforderungen**

Verträge mit Lieferanten enthalten verbindliche Sicherheitsanforderungen: - Informationssicherheits-Klauseln - Datenschutz-Anforderungen (DSGVO) - Audit-Rechte und Nachweispflichten - Incident-Notification-Pflichten - Subunternehmer-Regelungen

### **44.3.3 3.3 Cloud Security Assessment**

Cloud-Provider werden nach anerkannten Standards bewertet (ISO 27001, SOC 2, CSA STAR). Shared Responsibility Model wird dokumentiert und verstanden.

### **44.3.4 3.4 Datenklassifizierung und Cloud-Nutzung**

Die Speicherung und Verarbeitung von Daten in der Cloud richtet sich nach der Datenklassifizierung:  
- **Öffentlich:** Alle Cloud-Services erlaubt - **Intern:** Genehmigte Cloud-Services mit angemessenen Kontrollen - **Vertraulich:** Nur zertifizierte Cloud-Services mit Verschlüsselung - **Streng Vertraulich:** Nur On-Premise oder dedizierte Cloud mit erweiterten Kontrollen

### **44.3.5 3.5 Supplier Lifecycle Management**

Lieferanten werden über ihren gesamten Lebenszyklus verwaltet: - **Onboarding:** Security Assessment, Vertragsverhandlung - **Betrieb:** Kontinuierliches Monitoring, regelmäßige Reviews - **Offboarding:** Sichere Datenrückgabe/-löschung, Zugriffsentzug

### **44.3.6 3.6 Regelmäßige Supplier Reviews**

Kritische Lieferanten werden jährlich überprüft. Reviews umfassen Sicherheits-Compliance, Incident-Historie, Zertifizierungen und Performance.

### **44.3.7 3.7 Supply Chain Security**

Die Sicherheit der gesamten Lieferkette wird berücksichtigt. Lieferanten müssen Sicherheitsanforderungen an ihre Subunternehmer weitergeben.

### **44.3.8 3.8 Cloud Data Residency und Compliance**

Datenstandorte (Data Residency) werden dokumentiert und entsprechen regulatorischen Anforderungen (DSGVO, Schrems II).

## **44.4 4. Rollen und Verantwortlichkeiten**

### **44.4.1 RACI-Matrix: Lieferanten und Cloud Sicherheit**

Aktivität	CISO	Procurement	Legal	DPO	Business Owner	IT-Betrieb
Policy-Erstellung	R/A	C	C	C	I	C
Risk Assessment	R/A	C	C	C	C	C
Vertragsverhandlung	C	R	R/A	C	C	I
Security Review	R/A	I	I	C	C	C
Supplier Monitoring	A	C	I	I	C	R
Cloud Security Assessment	R/A	C	I	C	C	C
Offboarding	C	C	I	C	C	R/A

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

#### 44.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **Third-Party Risk Manager:** {{ meta.security.tprm\_manager }}
- **Cloud Security Architect:** {{ meta.security.cloud\_architect }}
- **Data Protection Officer:** {{ meta.dpo.name }}
- **Umsetzungsverantwortliche:** Procurement, Legal, IT-Betrieb
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit

### 44.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

#### 44.5.1 Zugehörige Richtlinien

- 0470\_Richtlinie\_Third\_Party\_Risk\_Assessment\_und\_Cloud\_Controls.md - Detaillierte Implementierungsrichtlinie
- 0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md - Data Classification Policy
- 0560\_Policy\_Datenschutz\_Schnittstellen.md - Data Protection Policy
- 0440\_Policy\_Business\_Continuity\_ICT\_Readiness.md - Business Continuity Policy

#### 44.5.2 Zugehörige Standards/Baselinses

- Third-Party Risk Assessment Framework
- Cloud Security Assessment Criteria
- Vertragliche Sicherheitsklauseln (Templates)
- Supplier Security Scorecard

#### 44.5.3 Zugehörige Prozesse

- Third-Party Risk Management Prozess
- Cloud Service Approval Prozess
- Supplier Review Prozess
- Supplier Offboarding Prozess

### 44.6 6. Compliance, Monitoring und Durchsetzung

#### 44.6.1 Messgrößen und KPIs

- Anzahl Lieferanten mit aktuellem Security Assessment (Ziel: 100% kritischer Lieferanten)
- Durchschnittlicher Supplier Security Score
- Anzahl Supplier Security Incidents
- Cloud Service Approval Rate
- Supplier Review Completion Rate (Ziel: 100% jährlich)
- Anzahl nicht-genehmigter Cloud-Services (Shadow IT)

#### 44.6.2 Nachweise und Evidence

- Third-Party Risk Assessments
- Supplier Security Scorecards
- Verträge mit Sicherheitsklauseln
- Cloud Security Assessments
- Supplier Review Reports
- Audit-Berichte zu Supplier Security

#### 44.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:

- **Nutzung nicht-genehmigter Cloud-Services:** Sofortige Deaktivierung, Untersuchung
- **Fehlende Risk Assessments:** Nachholung, Vertragsaussetzung
- **Supplier Security Incidents:** Incident Response, Vertragsüberprüfung
- **Wiederholte Verstöße:** Vertragsbeendigung, arbeitsrechtliche Konsequenzen

### 44.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und Business Owner genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet
- **Kompensationsmaßnahmen:** Ausnahmen erfordern alternative Sicherheitsmaßnahmen

### 44.8 8. Referenzen

#### 44.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy

- 0470\_Richtlinie\_Third\_Party\_Risk\_Assessment\_und\_Cloud\_Controls.md - Detailed Guideline
- 0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md - Data Classification Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

#### 44.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.5.19 - Information security in supplier relationships
  - ISO/IEC 27001:2022 Annex A.5.20 - Addressing information security within supplier agreements
  - ISO/IEC 27001:2022 Annex A.5.21 - Managing information security in the ICT supply chain
  - ISO/IEC 27001:2022 Annex A.5.22 - Monitoring, review and change management of supplier services
  - ISO/IEC 27001:2022 Annex A.5.23 - Information security for use of cloud services
  - ISO/IEC 27017 - Cloud Security Controls
  - ISO/IEC 27018 - Cloud Privacy
  - CSA STAR - Cloud Security Alliance Security, Trust & Assurance Registry
  - DSGVO (EU 2016/679) - Art. 28 - Auftragsverarbeitung
- 

**Genehmigt durch:**

{{ meta.management.ceo }}, Geschäftsführung  
Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

## Chapter 45

# Richtlinie: Third-Party Risk Assessment und Cloud Controls

Dokument-ID: 0470

## **Dokumenttyp:** Richtlinie (detailliert)

Zugehörige Policy: 0460\_Policy\_Lieferanten\_und\_Cloud\_Sicherheit.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.19, A.5.20, A.5.21, A.5.22, A.5.23

**Owner:** {{ meta.procurement.manager }}

Version: 1.0

**Status:** Freigegeben

### Klassifizierung: Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

## 45.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0460\_Policy\_Lieferanten\_und\_Cloud\_Sicherheit.md und definiert:

- Third-Party Risk Assessment Prozesse
- Cloud Security Controls und Compliance
- Lieferantenmanagement und -überwachung

**Geltungsbereich:** Alle Lieferanten und Cloud-Services bei AdminSend GmbH

## 45.2 2. Third-Party Risk Assessment

### 45.2.1 2.1 Lieferanten-Kategorisierung

## 45.2.2 2.2 Pre-Contract Assessment

**Phase 1: Initial Screening** - Fragebogen zu Sicherheitskontrollen - Zertifizierungen (ISO 27001, SOC 2) - Datenschutz-Compliance (DSGVO) - Finanzielle Stabilität

**Phase 2: Detailed Assessment (Kritisch/Hoch)** - Security-Audit oder On-Site-Visit - Penetration-Test-Berichte - Incident-Response-Fähigkeiten - Business Continuity Plans

**Phase 3: Contract Negotiation** - Security-Klauseln im Vertrag - SLAs für Sicherheit und Verfügbarkeit - Audit-Rechte - Incident-Notification-Pflichten

## 45.2.3 2.3 Ongoing Monitoring

**Frequenz:** - Kritisch: Quartalsweise Review - Hoch: Halbjährlich - Mittel: Jährlich - Niedrig: Bei Vertragsverlängerung

**Monitoring-Aktivitäten:** - Zertifizierungs-Status prüfen - Security-Incidents beim Lieferanten - Compliance-Berichte anfordern - Performance gegen SLAs

## 45.2.4 2.4 Offboarding

**Prozess:** 1. Datenrückgabe oder -löschung 2. Zugriffe widerrufen 3. Vertraulichkeitsverpflichtungen bestätigen 4. Abschlussdokumentation

# 45.3 3. Cloud Security Controls

## 45.3.1 3.1 Cloud Service Models

**IaaS (Infrastructure as a Service):** - Shared Responsibility Model - Kunde verantwortlich für OS, Anwendungen, Daten - Provider verantwortlich für Infrastruktur

**PaaS (Platform as a Service):** - Provider verantwortlich für Plattform - Kunde verantwortlich für Anwendungen, Daten

**SaaS (Software as a Service):** - Provider verantwortlich für alles außer Daten - Kunde verantwortlich für Daten und Zugriffskontrolle

## 45.3.2 3.2 Cloud Security Assessment

**Vor Cloud-Adoption:** - Cloud Security Posture Assessment - Data Residency und Compliance prüfen - Verschlüsselungsoptionen evaluieren - Backup und DR-Fähigkeiten

**Cloud Security Controls:** - Identity and Access Management (IAM) - Netzwerk-Segmentierung - Verschlüsselung (at rest, in transit) - Logging und Monitoring - Compliance-Zertifizierungen

## 45.3.3 3.3 Cloud Access Security Broker (CASB)

**Funktionen:** - Visibility in Cloud-Nutzung - Data Loss Prevention (DLP) - Threat Protection - Compliance-Monitoring

**CASB-System:** {{ meta.security.casb\_solution }}

#### **45.3.4 3.4 Multi-Cloud und Hybrid-Cloud**

**Governance:** - Einheitliche Security-Policies über alle Clouds - Zentrale Identity-Provider (SSO) - Konsistentes Monitoring

**Cloud-Provider:** - Primary: {{ meta.cloud.primary\_provider }} - Secondary: {{ meta.cloud.secondary\_provider }}

### **45.4 4. Vertragsmanagement**

#### **45.4.1 4.1 Security-Klauseln**

**Pflicht-Klauseln:** - Datenschutz und DSGVO-Compliance - Sicherheitskontrollen und -standards - Incident-Notification (innerhalb 24 Stunden) - Audit-Rechte - Datenrückgabe bei Vertragsende - Haftung bei Datenverletzungen

#### **45.4.2 4.2 Service Level Agreements (SLAs)**

**Security-SLAs:** - Verfügbarkeit (z.B. 99.9%) - Incident-Response-Zeit - Patch-Management-Zeitrahmen - Backup-Frequenz und -Retention

#### **45.4.3 4.3 Data Processing Agreements (DPA)**

**DSGVO-Anforderungen:** - Auftragsverarbeitungsvertrag (AVV) - Technische und organisatorische Maßnahmen (TOMs) - Sub-Processor-Liste - Datenübermittlung in Drittländer

### **45.5 5. Lieferanten-Risikomanagement**

#### **45.5.1 5.1 Risiko-Register**

**Dokumentation:** - Lieferant, Service, Kritikalität - Identifizierte Risiken - Mitigationsmaßnahmen - Residual Risk - Review-Datum

#### **45.5.2 5.2 Incident Management**

**Bei Lieferanten-Incidents:** 1. Benachrichtigung durch Lieferanten (SLA: 24h) 2. Impact-Assessment 3. Mitigationsmaßnahmen koordinieren 4. Eigene Kunden informieren (falls erforderlich) 5. Post-Incident-Review

#### **45.5.3 5.3 Business Continuity**

**Lieferanten-Ausfall-Szenarien:** - Alternative Lieferanten identifizieren - Exit-Strategie definieren - Daten-Portabilität sicherstellen

### **45.6 6. Compliance und Audit**

#### **45.6.1 6.1 Messgrößen (KPIs)**

Metrik	Zielwert
Lieferanten mit aktuellem Assessment	100%
Kritische Lieferanten mit ISO 27001	> 90%
SLA-Einhaltung	> 95%
Incident-Notification-Compliance	100%

## 45.6.2 6.2 Audit-Nachweise

- Lieferanten-Assessments
- Verträge mit Security-Klauseln
- SLA-Reports
- Incident-Dokumentation

## 45.7 7. Referenzen

### 45.7.1 Interne Dokumente

- 0460\_Policy\_Lieferanten\_und\_Cloud\_Sicherheit.md
- 0400\_Policy\_Incident\_Management.md

### 45.7.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.5.19 - Information security in supplier relationships
- ISO/IEC 27001:2022 Annex A.5.20 - Addressing information security within supplier agreements
- ISO/IEC 27001:2022 Annex A.5.21 - Managing information security in the ICT supply chain
- ISO/IEC 27001:2022 Annex A.5.22 - Monitoring, review and change management of supplier services
- ISO/IEC 27001:2022 Annex A.5.23 - Information security for use of cloud services

---

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 46

## Policy: Physische Sicherheit

**Dokument-ID:** 0480

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.7.1-A.7.4 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 46.1 1. Zweck

Diese Policy definiert die Grundsätze für physische Sicherheit der **AdminSend GmbH**. Sie stellt sicher, dass physischer Zugang zu Einrichtungen, Geräten und Informationen kontrolliert und überwacht wird, um unbefugten Zugriff, Diebstahl und Beschädigung zu verhindern.

### 46.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Einrichtungen:** Büros, Rechenzentren, Serverräume, Lager, Produktionsstätten
- **Assets:** IT-Equipment, Server, Netzwerkkomponenten, mobile Geräte, Dokumente
- **Personen:** Mitarbeiter, Besucher, Auftragnehmer, Lieferanten
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_) zulässig.

## **46.3 3. Grundsätze (Policy Statements)**

### **46.3.1 3.1 Perimeter-Sicherheit**

Physische Sicherheitsbereiche werden durch Perimeter-Sicherheit geschützt (Zäune, Mauern, Sicherheitstüren). Zutrittspunkte werden kontrolliert und überwacht.

### **46.3.2 3.2 Zutrittskontrolle**

Der Zutritt zu sensiblen Bereichen wird kontrolliert: - Elektronische Zutrittskontrollsysteme (Badge, Biometrie) - Besuchermanagement und Begleitpflicht - Protokollierung aller Zutritte - Regelmäßige Überprüfung von Zutrittsrechten

### **46.3.3 3.3 Sicherheitszonen**

Einrichtungen werden in Sicherheitszonen eingeteilt: - **Öffentlich:** Empfang, Besprechungsräume - **Intern:** Büros, Arbeitsplätze - **Eingeschränkt:** Serverräume, Rechenzentren - **Hochsicher:** Kritische Infrastruktur, Tresorräume

### **46.3.4 3.4 Videoüberwachung**

Kritische Bereiche werden videoüberwacht. Aufzeichnungen werden gemäß Datenschutzanforderungen gespeichert und geschützt.

### **46.3.5 3.5 Schutz vor Umweltgefahren**

IT-Equipment wird vor Umweltgefahrenen geschützt: - Brandschutz (Rauchmelder, Löschanlagen) - Klimatisierung und Temperaturüberwachung - Wasserschutz (Leckageerkennung) - Stromversorgung (USV, Notstromgeneratoren)

### **46.3.6 3.6 Sichere Entsorgung**

Physische Medien und Dokumente werden sicher entsorgt (Schreddern, Verbrennen, zertifizierte Entsorgung).

### **46.3.7 3.7 Clear Desk und Clear Screen**

Arbeitsplätze werden bei Abwesenheit aufgeräumt (Clear Desk). Bildschirme werden gesperrt (Clear Screen).

### **46.3.8 3.8 Equipment Security**

IT-Equipment wird vor Diebstahl geschützt (Kensington-Locks, Alarmanlagen, Inventarisierung).

## **46.4 4. Rollen und Verantwortlichkeiten**

### **46.4.1 RACI-Matrix: Physische Sicherheit**

Aktivität	CISO	Facility Management	Security	IT-Betrieb	HR
Policy-Erstellung	R/A	C	C	C	I
Zutrittskontrolle	C	R/A	R	I	C
Besuchermanagement	I	R/A	R	I	C
Videoüberwachung	C	R/A	R	I	C
Umweltschutz	C	R/A	I	C	I
Equipment Security	C	C	I	R/A	I
Compliance-Prüfung	R/A	C	C	I	I

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

#### 46.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **Facility Manager:** {{ meta.facility.manager }}
- **Security Manager:** {{ meta.security.physical\_security\_manager }}
- **Umsetzungsverantwortliche:** Facility Management, Security, IT-Betrieb
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit

### 46.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

#### 46.5.1 Zugehörige Richtlinien

- **0490\_Richtlinie\_Zutritt\_Besucher\_und\_Schutz\_von\_Equipment.md** - Detaillierte Implementierungsrichtlinie
- **0300\_Policy\_Asset\_Management.md** - Asset Management Policy
- **0560\_Policy\_Datenschutz\_Schnittstellen.md** - Data Protection Policy (Videoüberwachung)

#### 46.5.2 Zugehörige Standards/Baselinses

- Sicherheitszonen-Konzept
- Zutrittskontroll-Matrix
- Besuchermanagement-Prozess
- Videoüberwachungs-Richtlinie

#### 46.5.3 Zugehörige Prozesse

- Zutrittskontroll-Prozess
- Besuchermanagement-Prozess
- Incident Response bei physischen Sicherheitsvorfällen
- Equipment-Entsorgungsprozess

## 46.6 6. Compliance, Monitoring und Durchsetzung

### 46.6.1 Messgrößen und KPIs

- Anzahl unbefugter Zutrittsversuche
- Besucheranzahl und Compliance mit Begleitpflicht
- Anzahl physischer Sicherheitsvorfälle (Diebstahl, Einbruch)
- Zutrittskontroll-System-Verfügbarkeit (Ziel: 99.9%)
- Clear Desk/Clear Screen Compliance-Rate
- Anzahl verlorener oder gestohlenen Assets

### 46.6.2 Nachweise und Evidence

- Zutrittskontroll-Logs
- Besucherprotokolle
- Videoüberwachungs-Aufzeichnungen
- Sicherheitsvorfalls-Reports
- Facility-Audit-Berichte
- Equipment-Inventar

### 46.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt: -

**Unbefugter Zutritt:** Sofortige Eskalation, Untersuchung - **Tailgating (Mitschleusen):** Verwarnung, Nachschulung -

**Clear Desk/Screen-Verstöße:** Verwarnung, Nachschulung - **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen

## 46.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und Facility Manager genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet

## 46.8 8. Referenzen

### 46.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0490\_Richtlinie\_Zutritt\_Besucher\_und\_Schutz\_von\_Equipment.md - Detailed Guideline
- 0300\_Policy\_Asset\_Management.md - Asset Management Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

### 46.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.7.1 - Physical security perimeters
- ISO/IEC 27001:2022 Annex A.7.2 - Physical entry
- ISO/IEC 27001:2022 Annex A.7.3 - Securing offices, rooms and facilities

- ISO/IEC 27001:2022 Annex A.7.4 - Physical security monitoring
  - DSGVO (EU 2016/679) - Datenschutz bei Videoüberwachung
  - BSI IT-Grundschutz - Baustein INF.1 Allgemeines Gebäude
- 

**Genehmigt durch:**

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 47

## Richtlinie: Zutritt, Besucher und Schutz von Equipment

**Dokument-ID:** 0490

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0480\_Policy\_Physische\_Sicherheit.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.7.1, A.7.2, A.7.3, A.7.4

**Owner:** {{ meta.facilities.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 47.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0480\_Policy\_Physische\_Sicherheit.md und definiert:  
- Zutrittskontrollsysteme und -prozesse  
- Besuchermanagement  
- Physischer Schutz von IT-Equipment

**Geltungsbereich:** Alle Standorte von AdminSend GmbH

### 47.2 2. Sicherheitszonen

#### 47.2.1 2.1 Zonen-Klassifizierung

**Zone 1 (Öffentlich):** - Empfangsbereich, Lobby - Keine Zutrittskontrolle - Videoüberwachung

**Zone 2 (Intern):** - Bürobereiche, Besprechungsräume - Zutrittskarte erforderlich - Mitarbeiter und registrierte Besucher

**Zone 3 (Eingeschränkt):** - Serverräume, Rechenzentren - Zusätzliche Authentifizierung (PIN, Biometrie) - Nur autorisiertes Personal

**Zone 4 (Hochsicherheit):** - Kritische Infrastruktur - Vier-Augen-Prinzip - Videoüberwachung und Logging

## 47.3 3. Zutrittskontrollsyste

### 47.3.1 3.1 Zutrittskarten

**Kartentyp:** RFID-Karten mit Foto

**Ausgabe:** Bei Onboarding durch HR

**Gültigkeit:** Bis Vertragsende

**Kartenverlust:** 1. Sofortige Meldung an Security 2. Karte sperren (innerhalb 15 Minuten) 3. Neue Karte ausstellen 4. Dokumentation

### 47.3.2 3.2 Biometrische Authentifizierung

**Für Zone 3/4:** - Fingerabdruck-Scanner - Iris-Scanner (optional) - Datenschutz-konform (DS-GVO)

### 47.3.3 3.3 Zugriffsprotokolle

**Logging:** - Alle Zutrittsversuche (Erfolg und Fehler) - Timestamp, Person, Tür/Zone - Retention: {{ meta.retention.access\_years }} Jahre

**Monitoring:** - Alerts bei unautorisierten Zugriffsversuchen - Alerts bei Zugriff außerhalb Geschäftszonen (Zone 3/4)

## 47.4 4. Besuchermanagement

### 47.4.1 4.1 Besucheranmeldung

**Prozess:** 1. Gastgeber meldet Besucher vorab an (E-Mail, Portal) 2. Besucher meldet sich am Empfang 3. Ausweis-Kontrolle (Personalausweis, Führerschein) 4. Besucherausweis ausgeben 5. Gastgeber abholen

**Besucherausweis:** - Temporäre RFID-Karte - Gültigkeit: 1 Tag - Automatische Deaktivierung nach Ablauf

### 47.4.2 4.2 Begleitung

**Pflicht:** - Besucher müssen jederzeit begleitet werden - Keine unbeaufsichtigten Besucher in Zone 2/3/4 - Gastgeber verantwortlich

**Ausnahmen:** - Langzeit-Auftragnehmer mit eigenem Badge - Nach Background-Check und NDA

### 47.4.3 4.3 Besucherprotokoll

**Dokumentation:** - Name, Firma, Ausweisnummer - Gastgeber, Zweck des Besuchs - Ein- und Austrittszeit - Retention: {{ meta.retention.visitor\_years }} Jahre

## 47.5 5. Physischer Schutz von Equipment

### 47.5.1 5.1 Serverräume und Rechenzentren

**Anforderungen:** - Klimatisierung (18-27°C, 40-60% Luftfeuchtigkeit) - Brandmeldeanlage und Löschsystem - Unterbrechungsfreie Stromversorgung (USV) - Notstromgenerator - Wassersensoren (Leckage-Erkennung)

**Zutrittskontrolle:** - Zone 3 oder 4 - Logging aller Zutritte - Videoüberwachung

### 47.5.2 5.2 Arbeitsplätze

**Clean Desk Policy:** - Keine vertraulichen Dokumente auf Schreibtisch (Feierabend) - Bildschirmsperre bei Abwesenheit - Abschließbare Schränke für vertrauliche Unterlagen

**Kensington-Locks:** - Pflicht für Laptops in Büros - Diebstahlschutz

### 47.5.3 5.3 Mobile Geräte

**Sicherheitsanforderungen:** - Verschlüsselung (BitLocker, FileVault) - Remote Wipe-Fähigkeit (MDM) - Keine vertraulichen Daten lokal (Cloud-Storage bevorzugen)

**Bei Verlust:** 1. Sofortige Meldung an IT-Support 2. Remote Wipe auslösen 3. Incident-Ticket erstellen 4. Polizeimeldung (bei Diebstahl)

## 47.6 6. Videoüberwachung

### 47.6.1 6.1 Überwachte Bereiche

**Kameras:** - Eingänge und Ausgänge - Serverräume (Zone 3/4) - Parkplätze - Keine Überwachung in Büros, Toiletten, Umkleiden

### 47.6.2 6.2 Datenschutz

**DSGVO-Compliance:** - Hinweisschilder auf Videoüberwachung - Zweckbindung (Sicherheit, Zutrittskontrolle) - Zugriff nur für autorisiertes Personal - Retention: 30 Tage (dann automatische Löschung)

## 47.7 7. Notfallzugang

### 47.7.1 7.1 Break-Glass-Verfahren

**Für Notfälle:** - Physischer Schlüssel in versiegeltem Umschlag - Aufbewahrung in Safe - Nutzung nur bei Notfällen (Feuer, medizinischer Notfall) - Dokumentation jeder Nutzung

### 47.7.2 7.2 Evakuierung

**Evakuierungsplan:** - Fluchtwege ausgeschildert - Sammelplätze definiert - Regelmäßige Evakuierungsübungen (jährlich)

## 47.8 8. Compliance und Audit

### 47.8.1 8.1 Messgrößen (KPIs)

Metrik	Zielwert
Unbegleitete Besucher	0
Zutrittskarten-Verluste	< 5 pro Jahr
Clean-Desk-Compliance	> 90%
Evakuierungsübungen	1 pro Jahr

### 47.8.2 8.2 Audit-Nachweise

- Zutrittsprotokolle
- Besucherprotokolle
- Videoaufzeichnungen (30 Tage)
- Evakuierungsübungs-Protokolle

## 47.9 9. Referenzen

### 47.9.1 Interne Dokumente

- 0480\_Policy\_Physische\_Sicherheit.md
- 0300\_Policy\_Asset\_Management.md

### 47.9.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.7.1 - Physical security perimeters
- ISO/IEC 27001:2022 Annex A.7.2 - Physical entry
- ISO/IEC 27001:2022 Annex A.7.3 - Securing offices, rooms and facilities
- ISO/IEC 27001:2022 Annex A.7.4 - Physical security monitoring

---

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 48

## Policy: Mobile Device und Remote Work

**Dokument-ID:** 0500

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.6.7, A.6.8, A.8.9 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 48.1 1. Zweck

Diese Policy definiert die Grundsätze für Mobile Device Management und Remote Work der **AdminSend GmbH**. Sie stellt sicher, dass mobile Geräte und Remote-Zugriffe sicher verwaltet werden und den Sicherheitsanforderungen der Organisation entsprechen.

### 48.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Geräte:** Laptops, Smartphones, Tablets, Wearables (unternehmenseigen und BYOD)
- **Zugriffsmethoden:** VPN, Remote Desktop, Cloud-Services, Mobile Apps
- **Personen:** Alle Mitarbeiter, Auftragnehmer mit Remote-Zugriff
- **Standorte:** {{ netbox.site.name }}, Home Office, öffentliche Orte, Reisen

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_) zulässig.

## **48.3 3. Grundsätze (Policy Statements)**

### **48.3.1 3.1 Mobile Device Management (MDM)**

Alle mobilen Geräte mit Zugriff auf Unternehmensressourcen werden über ein MDM-System verwaltet. MDM ermöglicht Konfiguration, Monitoring und Remote-Wipe.

### **48.3.2 3.2 BYOD (Bring Your Own Device)**

Private Geräte dürfen nur nach Genehmigung und Enrollment im MDM für geschäftliche Zwecke genutzt werden. BYOD-Geräte unterliegen denselben Sicherheitsanforderungen wie Unternehmensgeräte.

### **48.3.3 3.3 Device Encryption**

Alle mobilen Geräte müssen vollständig verschlüsselt sein (Full Disk Encryption). Verschlüsselung wird über MDM erzwungen und überwacht.

### **48.3.4 3.4 Secure Remote Access**

Remote-Zugriff auf Unternehmensressourcen erfolgt ausschließlich über sichere Kanäle: - VPN mit Multi-Faktor-Authentisierung - Zero Trust Network Access (ZTNA) - Sichere Remote Desktop Lösungen

### **48.3.5 3.5 Device Compliance**

Mobile Geräte müssen Compliance-Anforderungen erfüllen: - Aktuelle Betriebssystem-Version - Installierte Sicherheits-Updates - Aktivierte Bildschirmsperre - Keine Jailbreak/Root - Installierte Endpoint-Security-Software

### **48.3.6 3.6 Lost/Stolen Device Response**

Bei Verlust oder Diebstahl mobiler Geräte wird sofort ein Incident gemeldet. Remote-Wipe wird durchgeführt, um Datenverlust zu verhindern.

### **48.3.7 3.7 Public Wi-Fi und Netzwerksicherheit**

Nutzung öffentlicher Wi-Fi-Netzwerke ist nur über VPN gestattet. Unverschlüsselte Verbindungen zu Unternehmensressourcen sind untersagt.

### **48.3.8 3.8 Remote Work Security**

Remote-Arbeitsplätze müssen Sicherheitsanforderungen erfüllen: - Sichere Netzwerkverbindung - Physische Sicherheit (Bildschirmsperre, Clear Desk) - Keine Weitergabe von Zugangsdaten - Compliance mit Acceptable Use Policy

## **48.4 4. Rollen und Verantwortlichkeiten**

### **48.4.1 RACI-Matrix: Mobile Device und Remote Work**

Aktivität	CISO	IT-Betrieb	MDM Administrator	Mitarbeiter	HR
Policy-Erstellung	R/A	C	C	I	C
MDM-Betrieb	A	R	R	I	I
Device Enrollment	I	C	R	R/A	I
Compliance-Monitoring	A	C	R	I	I
Lost Device Response	A	R	R	R	C
Remote Access Provisioning	C	R/A	C	I	I
Security Training	A	I	I	R	R

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

#### 48.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **MDM Administrator:** {{ meta.it.mdm\_admin }}
- **Remote Access Manager:** {{ meta.it.remote\_access\_manager }}
- **Umsetzungsverantwortliche:** IT-Betrieb, Mitarbeiter
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit

### 48.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

#### 48.5.1 Zugehörige Richtlinien

- **0510\_Richtlinie\_MDM\_BringYourOwnDevice\_und\_Remote\_Access.md** - Detaillierte Implementierungsrichtlinie
- **0200\_Policy\_Akzeptable\_Nutzung\_IT.md** - Acceptable Use Policy
- **0240\_Policy\_Authentisierung\_und\_Passwoerter.md** - Authentication Policy
- **0620\_Policy\_Endpoint\_Security.md** - Endpoint Security Policy

#### 48.5.2 Zugehörige Standards/Baselines

- MDM-Konfigurationsstandards
- Device Compliance Requirements
- BYOD-Richtlinie
- Remote Access Standards

### 48.5.3 Zugehörige Prozesse

- Device Enrollment Prozess
- Lost/Stolen Device Response Prozess
- Remote Access Provisioning Prozess
- BYOD Approval Prozess

## 48.6 6. Compliance, Monitoring und Durchsetzung

### 48.6.1 Messgrößen und KPIs

- MDM Enrollment Rate (Ziel: 100% mobiler Geräte)
- Device Compliance Rate (Ziel: 95%)
- Anzahl nicht-compliant Geräte
- Durchschnittliche Zeit zur Remote-Wipe bei Lost Devices
- VPN-Nutzungsrate bei Remote Work
- Anzahl Lost/Stolen Device Incidents

### 48.6.2 Nachweise und Evidence

- MDM-Enrollment-Status
- Device Compliance Reports
- Remote Access Logs
- Lost Device Incident Reports
- BYOD Approval Dokumentation
- Security Training Nachweise

### 48.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:

- **Nicht-enrollierte Geräte:** Zugriffssperre, Enrollment-Pflicht
- **Non-Compliance:** Zugriffsbeschränkung bis Remediation
- **Nicht gemeldeter Geräteverlust:** Untersuchung, Disziplinarmaßnahmen
- **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen

## 48.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet
- **Kompensationsmaßnahmen:** Ausnahmen erfordern alternative Sicherheitsmaßnahmen

## 48.8 8. Referenzen

### 48.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy

- 0510\_Richtlinie\_MDM\_BringYourOwnDevice\_und\_Remote\_Access.md - Detailed Guideline
- 0620\_Policy\_Endpoint\_Security.md - Endpoint Security Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

#### 48.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.6.7 - Remote working
  - ISO/IEC 27001:2022 Annex A.6.8 - Information security event reporting
  - ISO/IEC 27001:2022 Annex A.8.9 - Configuration management
  - NIST SP 800-46 - Guide to Enterprise Telework, Remote Access, and BYOD Security
  - DSGVO (EU 2016/679) - Datenschutz bei BYOD und Remote Work
- 

**Genehmigt durch:**

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 49

## Richtlinie: MDM, Bring Your Own Device und Remote Access

**Dokument-ID:** 0510

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0500\_Policy\_Mobile\_Device\_und\_Remote\_Work.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.6.7, A.8.9

**Owner:** {{ meta.it\_operations.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 49.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0500\_Policy\_Mobile\_Device\_und\_Remote\_Work.md und definiert:  
- Mobile Device Management (MDM) Anforderungen  
- BYOD-Richtlinien und -Prozesse  
- Remote-Access-Kontrollen

**Geltungsbereich:** Alle mobilen Geräte und Remote-Zugriffe bei **AdminSend GmbH**

### 49.2 2. Mobile Device Management (MDM)

#### 49.2.1 2.1 MDM-System

**Plattform:** {{ meta.mdm.system }} (z.B. Microsoft Intune, Jamf, MobileIron)

**Verwaltete Geräte:** - Unternehmenseigene Smartphones und Tablets - BYOD-Geräte mit Unternehmenszugriff - Laptops (optional, je nach MDM-Fähigkeit)

#### 49.2.2 2.2 MDM-Enrollment

**Prozess:** 1. Gerät erhalten oder BYOD-Antrag genehmigt 2. MDM-App installieren 3. Enrollment durchführen 4. Compliance-Checks bestehen 5. Unternehmenszugriff aktiviert

**Pflicht-Enrollment:** - Alle unternehmenseigenen Geräte - Alle BYOD-Geräte mit E-Mail-Zugriff oder Unternehmens-Apps

### 49.2.3 2.3 MDM-Policies

**Erzwungene Einstellungen:** - GerätEVERSCHLÜSSELUNG aktiviert - PIN/Passcode (min. 6 Zeichen) oder Biometrie - Automatische Bildschirmsperre (5 Minuten) - OS-Updates innerhalb 30 Tage - Jailbreak/Root-Detection

**Verbotene Aktivitäten:** - Jailbreak oder Rooting - Installation aus unbekannten Quellen - Deaktivierung von Sicherheitsfeatures

### 49.2.4 2.4 Compliance-Checks

**Automatische Prüfungen:** - OS-Version aktuell? - Verschlüsselung aktiv? - Jailbreak/Root erkannt? - Malware erkannt?

**Bei Non-Compliance:** - Warnung an Nutzer (24 Stunden Frist) - Eingeschränkter Zugriff - Vollständige Sperrung nach 7 Tagen

## 49.3 3. BYOD (Bring Your Own Device)

### 49.3.1 3.1 BYOD-Berechtigung

**Voraussetzungen:** - Antrag über Self-Service-Portal - Genehmigung durch Vorgesetzten - BYOD-Vereinbarung unterschreiben - MDM-Enrollment

**Berechtigte Geräte:** - Smartphones (iOS, Android) - Tablets (iOS, Android) - Laptops (nach Einzelfallprüfung)

### 49.3.2 3.2 BYOD-Vereinbarung

**Inhalte:** - Nutzungsbedingungen - Sicherheitsanforderungen - MDM-Enrollment-Pflicht - Remote-Wipe-Zustimmung - Datenschutz (Trennung privat/geschäftlich) - Haftung bei Verlust

### 49.3.3 3.3 Containerisierung

**Technologie:** - Separate Container für geschäftliche Daten - Verschlüsselte Container - Keine Vermischung privat/geschäftlich

**Beispiele:** - iOS: Managed Apps - Android: Work Profile - Windows: Windows Information Protection (WIP)

### 49.3.4 3.4 BYOD-Offboarding

**Bei Vertragsende oder BYOD-Beendigung:** 1. Remote Wipe des geschäftlichen Containers  
2. Entfernung von Unternehmens-Apps  
3. Widerruf von Zertifikaten  
4. MDM-Unenrollment  
5. Private Daten bleiben erhalten

## 49.4 4. Remote Access

### 49.4.1 4.1 VPN-Zugriff

**VPN-System:** {{ meta.network.vpn\_solution }}

**Anforderungen:** - Multi-Faktor-Authentifizierung (MFA) - Endpoint-Compliance-Check vor Verbindung - Split-Tunneling verboten (Full-Tunnel) - Session-Timeout: 8 Stunden

**VPN-Clients:** - Unternehmens-genehmigte Clients - Automatische Updates - Kill-Switch aktiviert

### 49.4.2 4.2 Zero Trust Network Access (ZTNA)

**Prinzipien:** - Never Trust, Always Verify - Least Privilege Access - Micro-Segmentation

**Implementierung:** - Identity-basierte Zugriffskontrolle - Device Posture Checks - Continuous Authentication

### 49.4.3 4.3 Remote Desktop

**Technologien:** - RDP über VPN (Windows) - SSH über VPN (Linux) - Citrix/VMware Horizon (Virtual Desktops)

**Sicherheitskontrollen:** - MFA für Remote Desktop - Session-Recording (privilegierte Zugriffe) - Idle-Timeout: 30 Minuten

## 49.5 5. Remote Work Security

### 49.5.1 5.1 Home Office Anforderungen

**Netzwerk:** - Sicheres WLAN (WPA3 oder WPA2) - Keine öffentlichen WLANs ohne VPN - Router-Firmware aktuell

**Arbeitsplatz:** - Privater Arbeitsbereich (keine Einsicht Dritter) - Bildschirmsperre bei Abwesenheit - Keine Nutzung durch Familienmitglieder

### 49.5.2 5.2 Öffentliche Orte

**Erlaubt mit Einschränkungen:** - Arbeit in Cafés, Flughäfen, Hotels - VPN verpflichtend - Privacy-Screen für Laptop - Keine vertraulichen Gespräche

**Verboten:** - Öffentliche Computer (Internet-Cafés) - Ungesicherte WLANs ohne VPN - Unbeaufsichtigtes Gerät

### 49.5.3 5.3 Reisen

**Internationale Reisen:** - Meldung an IT-Security (Hochrisiko-Länder) - Reise-Laptop ohne vertrauliche Daten - Verschlüsselung verpflichtend - Keine Nutzung lokaler USB-Sticks

## 49.6 6. Mobile Application Management (MAM)

### 49.6.1 6.1 Genehmigte Apps

**Unternehmens-Apps:** - E-Mail ({{ meta.email.mobile\_app }}) - Collaboration ({{ meta.collaboration.mobile\_app }}) - VPN-Client - Authenticator-App

**Genehmigungsprozess:** - Antrag über IT-Portal - Security-Review - Freigabe durch IT-Security

### 49.6.2 6.2 App-Wrapping

**Für unternehmenseigene Apps:** - MDM-Policies in App integrieren - Verschlüsselung erzwingen  
- Copy/Paste-Kontrolle

## 49.7 7. Incident Response

### 49.7.1 7.1 Geräteverlust

**Sofortmaßnahmen:** 1. Meldung an IT-Support ({{ meta.support.phone }}) 2. Remote Wipe auslösen (innerhalb 1 Stunde) 3. Passwörter ändern 4. Incident-Ticket erstellen 5. Polizeimeldung (bei Diebstahl)

### 49.7.2 7.2 Kompromittierung

**Bei Verdacht auf Malware:** 1. Gerät vom Netzwerk trennen 2. IT-Security informieren 3. Forensische Analyse (falls erforderlich) 4. Gerät neu aufsetzen 5. Lessons Learned

## 49.8 8. Compliance und Audit

### 49.8.1 8.1 Messgrößen (KPIs)

Metrik	Zielwert
MDM-Enrollment-Rate	100%
Compliance-Rate	> 95%
OS-Update-Rate (30 Tage)	> 90%
Remote-Wipe-Success-Rate	100%

### 49.8.2 8.2 Audit-Nachweise

- MDM-Enrollment-Logs
- Compliance-Reports
- BYOD-Vereinbarungen
- Remote-Access-Logs

## 49.9 9. Referenzen

### 49.9.1 Interne Dokumente

- 0500\_Policy\_Mobile\_Device\_und\_Remote\_Work.md

- 0250\_Richtlinie\_MFA\_Passwortregeln\_und\_Session\_Management.md

#### 49.9.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.6.7 - Remote working
- ISO/IEC 27001:2022 Annex A.8.9 - Configuration management
- NIST SP 800-124 - Guidelines for Managing the Security of Mobile Devices

---

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 50

## Policy: HR Security

**Dokument-ID:** 0520

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.6.1-A.6.4 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 50.1 1. Zweck

Diese Policy definiert die Grundsätze für HR Security der **AdminSend GmbH**. Sie stellt sicher, dass Sicherheitsverantwortlichkeiten über den gesamten Beschäftigungslebenszyklus verstanden und erfüllt werden - von der Einstellung bis zur Beendigung des Arbeitsverhältnisses.

### 50.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Personen:** Alle Mitarbeiter, Auftragnehmer, Zeitarbeiter, Praktikanten
- **Lebenszyklus:** Pre-Employment, Onboarding, Employment, Offboarding
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_zulässig.

## 50.3 3. Grundsätze (Policy Statements)

### 50.3.1 3.1 Pre-Employment Screening

Vor Einstellung werden angemessene Background Checks durchgeführt (Referenzen, Qualifikationen, ggf. Führungszeugnis). Das Screening richtet sich nach Rolle und Schutzbedarf.

### 50.3.2 3.2 Vertragliche Sicherheitsverpflichtungen

Arbeitsverträge enthalten Sicherheitsklauseln: - Vertraulichkeitsvereinbarungen (NDA) - Acceptable Use Policy Acknowledgement - Datenschutzverpflichtungen - Intellectual Property Rights

### 50.3.3 3.3 Security Awareness und Training

Alle Mitarbeiter durchlaufen Security Awareness Training: - **Onboarding:** Initiales Security Training - **Jährlich:** Auffrischungstraining - **Rollenspezifisch:** Zusätzliches Training für privilegierte Rollen

### 50.3.4 3.4 Joiner-Mover-Leaver-Prozess

Sicherheitsrelevante Aktivitäten werden im Beschäftigungslebenszyklus durchgeführt: - **Joiner:** Zugriffsvergabe, Training, Equipment-Ausgabe - **Mover:** Zugriffsanpassung bei Rollenwechsel - **Leaver:** Zugriffsentzug, Equipment-Rückgabe, Exit-Interview

### 50.3.5 3.5 Disziplinarverfahren

Sicherheitsverstöße werden nach definierten Disziplinarverfahren behandelt. Verstöße werden dokumentiert und können zu arbeitsrechtlichen Konsequenzen führen.

### 50.3.6 3.6 Verantwortlichkeiten und Pflichten

Mitarbeiter sind verpflichtet: - Sicherheitsrichtlinien einzuhalten - Sicherheitsvorfälle zu melden - An Security Training teilzunehmen - Vertraulichkeit zu wahren

### 50.3.7 3.7 Privilegierte Rollen

Mitarbeiter mit privilegierten Zugriffen unterliegen erweiterten Anforderungen: - Erweiterte Background Checks - Zusätzliches Security Training - Regelmäßige Rezertifizierung - Strikte Überwachung

### 50.3.8 3.8 Offboarding und Zugriffsentzug

Bei Beendigung des Arbeitsverhältnisses werden alle Zugriffe unverzüglich entzogen: - IT-Zugriffe deaktiviert (Ziel: < 1 Tag) - Equipment zurückgegeben - Vertraulichkeitsverpflichtungen erneuert - Exit-Interview durchgeführt

## 50.4 4. Rollen und Verantwortlichkeiten

### 50.4.1 RACI-Matrix: HR Security

Aktivität	CISO	HR	Hiring Manager	IT-Betrieb	Legal
Policy-Erstellung	R/A	C	C	I	C
Background Checks	C	R/A	C	I	C
Vertragsklauseln	C	R	I	I	R/A
Security Training	R/A	C	I	C	I
Joiner Process	C	R	R/A	R	I
Mover Process	C	R	R/A	R	I
Leaver Process	C	R/A	C	R	I
Disziplinarverfahren	C	R/A	C	I	C

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

#### 50.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **HR Manager:** {{ meta.hr.manager }}
- **Security Awareness Manager:** {{ meta.security.awareness\_manager }}
- **Umsetzungsverantwortliche:** HR, Hiring Manager, IT-Betrieb
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit

### 50.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

#### 50.5.1 Zugehörige Richtlinien

- [0530\\_Richtlinie\\_HR\\_Onboarding\\_Rollenwechsel\\_Offboarding.md](#) - Detaillierte Implementierungsrichtlinie
- [0220\\_Policy\\_Zugriffssteuerung\\_und\\_Identitätsmanagement.md](#) - Access Control Policy
- [0200\\_Policy\\_Akzeptable\\_Nutzung\\_IT.md](#) - Acceptable Use Policy
- [0120\\_ISMS\\_Schulung\\_Awareness\\_und\\_Kompetenz.md](#) - Training and Awareness

#### 50.5.2 Zugehörige Standards/Baselins

- Background Check Requirements
- Vertragliche Sicherheitsklauseln (Templates)
- Security Training Curriculum
- Joiner-Mover-Leaver Checklists

#### 50.5.3 Zugehörige Prozesse

- Pre-Employment Screening Prozess
- Joiner-Mover-Leaver Prozess
- Security Training Prozess
- Disziplinarverfahren

## 50.6 6. Compliance, Monitoring und Durchsetzung

### 50.6.1 Messgrößen und KPIs

- Background Check Completion Rate (Ziel: 100%)
- Security Training Completion Rate (Ziel: 100% jährlich)
- Durchschnittliche Zeit zur Zugriffsvergabe (Joiner)
- Durchschnittliche Zeit zum Zugriffsentzug (Leaver) (Ziel: < 1 Tag)
- Anzahl Sicherheitsverstöße und Disziplinarverfahren
- NDA Signing Rate (Ziel: 100%)

### 50.6.2 Nachweise und Evidence

- Background Check Dokumentation
- Verträge mit Sicherheitsklauseln
- Security Training Nachweise
- Joiner-Mover-Leaver Checklists
- Disziplinarverfahren-Dokumentation
- Exit-Interview-Protokolle

### 50.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:

- **Fehlende Background Checks:** Nachholung vor Zugriffsvergabe - **Nicht absolviertes Training:** Zugriffsbeschränkung bis Nachholung - **Sicherheitsverstöße:** Disziplinarverfahren nach HR-Prozess - **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen bis Kündigung

## 50.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und HR Manager genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet

## 50.8 8. Referenzen

### 50.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0530\_Richtlinie\_HR\_Onboarding\_Rollenwechsel\_Offboarding.md - Detailed Guideline
- 0220\_Policy\_Zugriffssteuerung\_und\_Identitätsmanagement.md - Access Control Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

### 50.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.6.1 - Screening
- ISO/IEC 27001:2022 Annex A.6.2 - Terms and conditions of employment

- **ISO/IEC 27001:2022 Annex A.6.3** - Information security awareness, education and training
  - **ISO/IEC 27001:2022 Annex A.6.4** - Disciplinary process
  - Arbeitsrechtliche Vorgaben (Deutschland)
  - DSGVO (EU 2016/679) - Datenschutz bei Background Checks
- 

**Genehmigt durch:**

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 51

## Richtlinie: HR Security - Onboarding, Rollenwechsel, Offboarding

**Dokument-ID:** 0530

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0520\_Policy\_HR\_Security.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.6.1, A.6.2, A.6.3, A.6.4

**Owner:** {{ meta.hr.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Vertraulich

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 51.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0520\_Policy\_HR\_Security.md und definiert: - Security-Aspekte im HR-Lifecycle - Onboarding, Rollenwechsel und Offboarding-Prozesse - Background-Checks und Vertraulichkeitsverpflichtungen

**Geltungsbereich:** Alle Mitarbeiter, Auftragnehmer und Dritte bei **AdminSend GmbH**

### 51.2 2. Pre-Employment

#### 51.2.1 2.1 Background Checks

**Standard-Mitarbeiter:** - Identitätsprüfung (Personalausweis) - Referenzen prüfen (2 Referenzen)  
- Bildungsabschlüsse verifizieren - Arbeitserlaubnis prüfen

**Privilegierte Rollen:** - Erweiterte Background-Checks - Führungszeugnis - Kreditwürdigkeit (bei Finanzzugriff) - Social Media Screening (optional)

**Externe Auftragnehmer:** - Firmen-Background-Check - NDA vor Zugriff - Sponsor-Verantwortung

## **51.2.2 2.2 Arbeitsvertrag**

**Security-Klauseln:** - Vertraulichkeitsverpflichtung - Acceptable Use Policy - Intellectual Property Rights - Post-Employment-Verpflichtungen

## **51.3 3. Onboarding**

### **51.3.1 3.1 Erster Arbeitstag**

**HR-Aktivitäten:** 1. Willkommens-Paket übergeben 2. Arbeitsvertrag unterschreiben 3. Security-Policies bestätigen 4. Notfallkontakte erfassen

**IT-Aktivitäten:** 1. Account-Erstellung (siehe 0230\_Richtlinie\_IAM) 2. Hardware-Ausgabe 3. IT-Einweisung 4. MFA-Registrierung

### **51.3.2 3.2 Security-Schulungen**

**Pflicht-Schulungen (Erste Woche):** - Information Security Awareness (2 Stunden) - Data Protection / DSGVO (1 Stunde) - Acceptable Use Policy (30 Minuten) - Phishing-Awareness (30 Minuten)

**Bestätigung:** - Quiz (Bestehensgrenze: 80%) - Unterschrift auf Schulungsnachweis

### **51.3.3 3.3 Rollenspezifische Schulungen**

**Entwickler:** - Secure Coding Training - OWASP Top 10

**Administratoren:** - Privileged Access Management - Incident Response

**HR/Finance:** - Data Privacy - Social Engineering Awareness

## **51.4 4. Rollenwechsel (Mover)**

### **51.4.1 4.1 interner Wechsel**

**HR-Prozess:** 1. Neue Rolle in HR-System aktualisieren 2. Alter und neuer Vorgesetzter informieren 3. IT-Ticket für Zugriffsänderungen

**IT-Prozess:** 1. Alte Zugriffe entziehen 2. Neue Zugriffe bereitstellen 3. Hardware anpassen (falls erforderlich) 4. Dokumentation aktualisieren

**Details:** Siehe 0230\_Richtlinie\_IAM

### **51.4.2 4.2 Beförderungen**

**Zusätzliche Prüfungen:** - Bei privilegierten Rollen: Erweiterter Background-Check - Security-Schulungen für neue Verantwortung - Vier-Augen-Prinzip bei kritischen Zugriffen

## 51.5 5. Offboarding

### 51.5.1 5.1 Geplantes Ausscheiden

**2 Wochen vor Austritt:** - Wissenstransfer planen - Übergabe-Checkliste erstellen - Zugriffe reviewen

**Letzter Arbeitstag:** - Hardware-Rückgabe - Zutrittskarte abgeben - Exit-Interview - Account-Deaktivierung (End of Day)

**Nach Austritt:** - Account-Lösung (nach 30 Tagen) - E-Mail-Weiterleitung (30 Tage) - Daten-Archivierung

**Details:** Siehe 0230\_Richtlinie\_IAM

### 51.5.2 5.2 Ungeplantes Ausscheiden

**Sofortmaßnahmen (innerhalb 1 Stunde):** 1. Alle Accounts deaktivieren 2. VPN-Zugriff sperren 3. Zutrittskarte deaktivieren 4. Mobile Geräte remote löschen 5. Vorgesetzten und Security informieren

**Gründe:** - Kündigung aus wichtigem Grund - Sicherheitsvorfälle - Verdacht auf Datenmissbrauch

### 51.5.3 5.3 Post-Employment

**Vertraulichkeitsverpflichtung:** - Bleibt nach Austritt bestehen - Keine Weitergabe von Geschäftsgeheimnissen - Rückgabe aller Unterlagen

**Wiedereinstellung:** - Neuer Background-Check - Neue Security-Schulungen - Neue Accounts (keine Reaktivierung alter Accounts)

## 51.6 6. Vertraulichkeitsverpflichtungen

### 51.6.1 6.1 Non-Disclosure Agreement (NDA)

**Unterzeichnung:** - Bei Einstellung (im Arbeitsvertrag) - Bei Zugriff auf vertrauliche Projekte - Bei Auftragsverarbeitung (externe Dienstleister)

**Inhalte:** - Definition vertraulicher Informationen - Nutzungsbeschränkungen - Dauer der Verpflichtung - Konsequenzen bei Verstößen

### 51.6.2 6.2 Intellectual Property (IP)

**Regelung:** - Alle Arbeitsergebnisse gehören dem Unternehmen - Keine private Nutzung von Unternehmens-Code - Offenlegung von Erfindungen

## 51.7 7. Disziplinarmaßnahmen

### 51.7.1 7.1 Security-Verstöße

**Kategorien:** - **Leicht:** Unbeabsichtigte Verstöße (z.B. Passwort-Sharing) - **Mittel:** Fahrlässige Verstöße (z.B. Datenverlust durch Unachtsamkeit) - **Schwer:** Vorsätzliche Verstöße (z.B. Datendiebstahl)

**Maßnahmen:** - Leicht: Verwarnung, Nachschulung - Mittel: Schriftliche Abmahnung - Schwer: Kündigung, Strafanzeige

## 51.7.2 7.2 Prozess

1. Incident-Meldung
2. Untersuchung durch HR und Security
3. Anhörung des Mitarbeiters
4. Entscheidung über Maßnahmen
5. Dokumentation
6. Umsetzung

# 51.8 8. Externe Auftragnehmer

## 51.8.1 8.1 Onboarding

**Voraussetzungen:** - Vertrag mit Security-Klauseln - NDA unterschrieben - Background-Check (durch Auftragnehmer-Firma) - Interner Sponsor

**Zugriffe:** - Zeitlich befristet - Nur projektbezogen - Regelmäßige Rezertifizierung (quartalsweise)

## 51.8.2 8.2 Monitoring

**Erhöhte Überwachung:** - Zugriffe auf vertrauliche Daten - Privilegierte Aktivitäten - Datenexporte

## 51.8.3 8.3 Offboarding

**Bei Projektende:** - Sofortige Zugriffsentziehung - Datenrückgabe oder -löschung - Bestätigung der Vertraulichkeitsverpflichtung

# 51.9 9. Compliance und Audit

## 51.9.1 9.1 Messgrößen (KPIs)

Metrik	Zielwert
Background-Check-Completion	100%
Security-Schulung (Onboarding)	100%
Offboarding-Completion (am letzten Tag)	100%
NDA-Unterzeichnung	100%

## 51.9.2 9.2 Audit-Nachweise

- Background-Check-Dokumentation
- Schulungsnachweise
- NDA-Unterschriften
- Offboarding-Checklisten

## 51.10 10. Referenzen

### 51.10.1 Interne Dokumente

- 0520\_Policy\_HR\_Security.md
- 0230\_Richtlinie\_IAM\_Joiner\_Mover\_Leaver\_und\_Zugriffsantraege.md

### 51.10.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.6.1 - Screening
- ISO/IEC 27001:2022 Annex A.6.2 - Terms and conditions of employment
- ISO/IEC 27001:2022 Annex A.6.3 - Information security awareness, education and training
- ISO/IEC 27001:2022 Annex A.6.4 - Disciplinary process

---

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 52

## Policy: Konfiguration und Hardening

**Dokument-ID:** 0540

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.8.9, A.8.10 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 52.1 1. Zweck

Diese Policy definiert die Grundsätze für sichere Konfiguration und System-Hardening der **Admin-Send GmbH**. Sie stellt sicher, dass IT-Systeme sicher konfiguriert und gegen Angriffe gehärtet werden.

### 52.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Systeme:** Alle Server, Workstations, Netzwerkgeräte, Anwendungen, Cloud-Ressourcen
- **Umgebungen:** Produktion, Test, Entwicklung
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_zulässig).

## 52.3 3. Grundsätze (Policy Statements)

### 52.3.1 3.1 Security Baselines

Für alle Systemtypen existieren Security Baselines, die Mindestanforderungen an sichere Konfiguration definieren. Baselines basieren auf anerkannten Standards (CIS Benchmarks, BSI, Vendor Best Practices).

### 52.3.2 3.2 Secure by Default

Systeme werden mit sicheren Standardkonfigurationen deployed. Unsichere Default-Einstellungen werden geändert, unnötige Features deaktiviert.

### 52.3.3 3.3 Hardening-Maßnahmen

Systeme werden gehärtet: - Entfernung unnötiger Software und Services - Deaktivierung nicht benötigter Ports und Protokolle - Änderung von Default-Credentials - Minimierung der Angriffsfläche

### 52.3.4 3.4 Configuration Management

Konfigurationen werden zentral verwaltet und versioniert (Infrastructure as Code, Configuration Management Tools). Änderungen erfolgen kontrolliert über Change Management.

### 52.3.5 3.5 Configuration Drift Detection

Abweichungen von Security Baselines (Configuration Drift) werden automatisch erkannt und gemeldet. Nicht genehmigte Änderungen werden zurückgesetzt.

### 52.3.6 3.6 Least Functionality

Systeme werden nach dem Prinzip der geringsten Funktionalität konfiguriert. Nur erforderliche Funktionen und Services sind aktiviert.

### 52.3.7 3.7 Secure Configuration Reviews

Konfigurationen werden regelmäßig überprüft: - **Kritische Systeme:** Quartalsweise - **Wichtige Systeme:** Halbjährlich - **Standard-Systeme:** Jährlich

### 52.3.8 3.8 Dokumentation

Alle Konfigurationsabweichungen von Baselines werden dokumentiert und begründet. Dokumentation ist aktuell und nachvollziehbar.

## 52.4 4. Rollen und Verantwortlichkeiten

### 52.4.1 RACI-Matrix: Konfiguration und Hardening

Aktivität	CISO	IT-Betrieb	System Owner	Security Team	Change Management
Policy-Erstellung	R/A	C	C	C	I
Baseline-Erstellung	A	C	C	R	I
System-Hardening	C	R/A	C	C	I
Configuration Management	C	R/A	C	I	C
Drift Detection	A	C	I	R	I
Configuration Reviews	A	C	R	R	I
Compliance-Prüfung	R/A	C	C	C	I

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

#### 52.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **Configuration Manager:** {{ meta.it.config\_manager }}
- **Security Architect:** {{ meta.security.architect }}
- **Umsetzungsverantwortliche:** IT-Betrieb, System Owner
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit

### 52.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

#### 52.5.1 Zugehörige Richtlinien

- **0550\_Richtlinie\_Sicherheitsbaselines\_Hardening\_und\_Konfig\_Aenderungen.md**
  - Detaillierte Implementierungsrichtlinie
- **0360\_Policy\_Change\_und\_Release\_Management.md** - Change Management Policy
- **0340\_Policy\_Vulnerability\_und\_Patch\_Management.md** - Vulnerability Management Policy

#### 52.5.2 Zugehörige Standards/Baselinses

- Security Baselines (Windows, Linux, Network Devices, Cloud)
- Hardening Guides
- Configuration Management Standards
- Drift Detection Rules

### 52.5.3 Zugehörige Prozesse

- Configuration Management Prozess
- Hardening Prozess
- Configuration Review Prozess
- Drift Remediation Prozess

## 52.6 6. Compliance, Monitoring und Durchsetzung

### 52.6.1 Messgrößen und KPIs

- Baseline Compliance Rate (Ziel: 95%)
- Anzahl Configuration Drift Findings
- Durchschnittliche Zeit zur Drift-Remediation
- Configuration Review Completion Rate (Ziel: 100%)
- Anzahl Systeme mit Default-Credentials (Ziel: 0)
- Hardening Coverage (Ziel: 100% kritischer Systeme)

### 52.6.2 Nachweise und Evidence

- Security Baselines Dokumentation
- Configuration Management Logs
- Drift Detection Reports
- Configuration Review Reports
- Hardening Checklists
- Audit-Berichte zu Configuration Compliance

### 52.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:  
- **Nicht gehärtete Systeme:** Sofortige Remediation, Produktionssperre  
- **Configuration Drift:** Remediation nach Priorität  
- **Default-Credentials:** Sofortige Änderung, Incident Response  
- **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen

## 52.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und System Owner genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet
- **Kompensationsmaßnahmen:** Ausnahmen erfordern alternative Sicherheitsmaßnahmen

## 52.8 8. Referenzen

### 52.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy

- 0550\_Richtlinie\_Sicherheitsbaselines\_Hardening\_und\_Konfig\_Aenderungen.md - Detailed Guideline
- 0360\_Policy\_Change\_und\_Release\_Management.md - Change Management Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

## 52.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.8.9 - Configuration management
  - ISO/IEC 27001:2022 Annex A.8.10 - Information deletion
  - CIS Benchmarks - Center for Internet Security Configuration Benchmarks
  - NIST SP 800-123 - Guide to General Server Security
  - BSI IT-Grundschutz - Sicherheitsanforderungen
- 

### Genehmigt durch:

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

Nächster Review: {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 53

## Richtlinie: Sicherheitsbaselines, Hardening und Konfigurationsänderungen

**Dokument-ID:** 0550

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0540\_Policy\_Konfiguration\_und\_Hardening.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.8.9

**Owner:** {{ meta.it\_operations.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Vertraulich

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 53.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0540\_Policy\_Konfiguration\_und\_Hardening.md und definiert:

- Sicherheitsbaselines für verschiedene Systemtypen
- Hardening-Prozesse und -Standards
- Configuration Management und Change Control

**Geltungsbereich:** Alle IT-Systeme bei **AdminSend GmbH**

### 53.2 2. Sicherheitsbaselines

#### 53.2.1 2.1 Windows Server

**Baseline-Standard:** CIS Benchmark Level 1

**Kern-Anforderungen:** - Lokale Administrator-Accounts deaktivieren (außer Break-Glass) - Windows Firewall aktiviert - Windows Defender aktiviert - Automatische Updates aktiviert - SMBv1 deaktiviert - PowerShell Logging aktiviert - Audit-Policies konfiguriert

**Tools:** - Group Policy Objects (GPOs) - Microsoft Security Compliance Toolkit - CIS-CAT Pro

### **53.2.2 2.2 Linux Server**

**Baseline-Standard:** CIS Benchmark Level 1

**Kern-Anforderungen:** - Root-Login über SSH deaktiviert - SSH Key-based Authentication - Firewall (iptables/firewalld) aktiviert - SELinux/AppArmor aktiviert - Automatische Security-Updates  
- Unnötige Services deaktiviert - Audit-Daemon (auditd) aktiviert

**Tools:** - Ansible/Puppet für Konfigurationsmanagement - Lynis für Security-Audits

### **53.2.3 2.3 Netzwerkgeräte**

**Baseline-Standard:** Vendor Best Practices + CIS Benchmarks

**Kern-Anforderungen:** - Default-Passwörter geändert - SNMP v3 (oder deaktiviert) - Unused Ports deaktiviert - Management-Zugriff nur über dediziertes VLAN - Logging zu SIEM - NTP konfiguriert

### **53.2.4 2.4 Cloud-Workloads**

**Baseline-Standard:** Cloud Security Posture Management (CSPM)

**Azure:** - Azure Security Benchmark - Microsoft Defender for Cloud Empfehlungen

**AWS:** - AWS Foundational Security Best Practices - CIS AWS Foundations Benchmark

**GCP:** - CIS Google Cloud Platform Foundation Benchmark

## **53.3 3. Hardening-Prozess**

### **53.3.1 3.1 Build-Phase**

**Golden Images:** - Vorkonfigurierte, gehärtete Images - Regelmäßige Updates (monatlich) - Automatisierte Builds (CI/CD)

**Prozess:** 1. Base-Image (Vendor) 2. Hardening-Scripts anwenden 3. Security-Scan 4. Approval 5. Image-Repository

### **53.3.2 3.2 Deployment-Phase**

**Automatisierung:** - Infrastructure as Code (Terraform, ARM Templates) - Configuration Management (Ansible, Puppet, Chef) - Compliance-Checks vor Deployment

**Manuelle Schritte:** - Nur bei Ausnahmen - Dokumentation erforderlich - Post-Deployment-Verification

### **53.3.3 3.3 Maintenance-Phase**

**Regelmäßige Reviews:** - Quartalsweise Configuration-Audits - Drift-Detection (Abweichungen von Baseline) - Remediation von Non-Compliance

## 53.4 4. Configuration Management

### 53.4.1 4.1 Configuration Management Database (CMDB)

**System:** {{ meta.itsm.cmdb }}

**Dokumentierte Konfigurationen:** - System-Typ und -Version - Installierte Software - Netzwerk-Konfiguration - Security-Konfiguration - Baseline-Version

### 53.4.2 4.2 Configuration Baselines

**Baseline-Versionen:** - Major-Version: Bei signifikanten Änderungen - Minor-Version: Bei kleineren Updates - Patch-Version: Bei Security-Fixes

**Beispiel:** Windows-Server-Baseline v2.1.3

### 53.4.3 4.3 Drift Detection

**Monitoring:** - Automatische Scans (täglich) - Vergleich mit Baseline - Alerts bei Abweichungen

**Tools:** - Microsoft Defender for Cloud (Azure) - AWS Config (AWS) - Chef InSpec, Ansible Tower

**Remediation:** - Automatische Korrektur (wo möglich) - Manuelle Korrektur mit Ticket - Ausnahmen-Prozess (siehe Abschnitt 6)

## 53.5 5. Konfigurationsänderungen

### 53.5.1 5.1 Change-Prozess

**Alle Konfigurationsänderungen über Change Management:** - Change Request (RFC) erstellen - Security-Impact-Assessment - Testing in Dev/Test - CAB-Genehmigung - Implementation - Verification

**Details:** Siehe 0370\_Richtlinie\_Change\_Management

### 53.5.2 5.2 Emergency Changes

**Bei kritischen Security-Fixes:** - Beschleunigter Prozess - ECAB-Genehmigung - Nachträgliche Dokumentation

### 53.5.3 5.3 Configuration Backup

**Vor jeder Änderung:** - Backup der aktuellen Konfiguration - Versionierung - Rollback-Fähigkeit

**Retention:** {{ meta.retention.config\_years }} Jahre

## 53.6 6. Ausnahmen und Abweichungen

### 53.6.1 6.1 Ausnahmenprozess

**Antrag:** - Begründung (Business Justification) - Risikobewertung - Kompensationskontrollen - Zeitliche Befristung

**Genehmigung:** - CISO-Genehmigung erforderlich - Dokumentation im Ausnahmen-Register - Regelmäßiger Review (quartalsweise)

**Details:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md

### 53.6.2 6.2 Legacy-Systeme

**Für Systeme, die Baseline nicht erfüllen können:** - Kompensationskontrollen implementieren - Netzwerk-Isolation - Erhöhtes Monitoring - Migration-Plan erstellen

## 53.7 7. Compliance-Monitoring

### 53.7.1 7.1 Automated Compliance Scanning

**Tools:** - **Windows:** Microsoft Security Compliance Toolkit, CIS-CAT - **Linux:** Lynis, OpenSCAP - **Cloud:** Cloud Security Posture Management (CSPM) - **Network:** Nessus, Qualys

**Frequenz:** - Kritische Systeme: Wöchentlich - Standard-Systeme: Monatlich

### 53.7.2 7.2 Compliance-Reporting

**Monatlicher Compliance-Report:** - Compliance-Rate pro Baseline - Top Non-Compliance-Items - Trend-Analyse - Remediation-Status

**Ziel:** > 95% Compliance

### 53.7.3 7.3 Audit-Nachweise

- Baseline-Dokumente
- Compliance-Scan-Berichte
- Ausnahmen-Register
- Remediation-Tickets

## 53.8 8. Hardening-Standards

### 53.8.1 8.1 Referenz-Standards

**Primär:** - CIS Benchmarks (Center for Internet Security) - DISA STIGs (Defense Information Systems Agency Security Technical Implementation Guides) - Vendor Best Practices

**Sekundär:** - NIST Cybersecurity Framework - BSI IT-Grundschutz

### 53.8.2 8.2 Baseline-Dokumentation

**Für jede Baseline:** - Scope und Anwendungsbereich - Konfigurationseinstellungen (detailliert) - Begründung für jede Einstellung - Test-Prozeduren - Rollback-Prozeduren

**Speicherort:** {{ meta.documentation.baseline\_repo }}

## 53.9 9. Compliance und Audit

### 53.9.1 9.1 Messgrößen (KPIs)

Metrik	Zielwert
Baseline-Compliance-Rate	> 95%
Drift-Remediation-Zeit	< 7 Tage
Golden-Image-Aktualität	< 30 Tage
Ausnahmen mit aktuellem Review	100%

### 53.9.2 9.2 Audit-Nachweise

- Baseline-Dokumente
- Compliance-Scan-Berichte
- Configuration-Backups
- Change-Records

## 53.10 10. Referenzen

### 53.10.1 Interne Dokumente

- 0540\_Policy\_Konfiguration\_und\_Hardening.md
- 0370\_Richtlinie\_Change\_Management\_mit\_Sicherheitsfreigaben.md
- 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md

### 53.10.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.8.9 - Configuration management
- CIS Benchmarks - <https://www.cisecurity.org/cis-benchmarks/>
- NIST SP 800-70 - Security Configuration Checklists

---

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 54

## Policy: Datenschutz Schnittstellen

**Dokument-ID:** 0560

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.31-A.5.34 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 54.1 1. Zweck

Diese Policy definiert die Schnittstellen zwischen Informationssicherheit und Datenschutz der **AdminSend GmbH**. Sie stellt sicher, dass ISMS und Datenschutzanforderungen aufeinander abgestimmt und koordiniert werden.

### 54.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Daten:** Alle personenbezogenen Daten gemäß DSGVO
- **Prozesse:** Alle Verarbeitungstätigkeiten personenbezogener Daten
- **Schnittstellen:** ISMS – Datenschutz-Management-System
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_) zulässig.

## **54.3 3. Grundsätze (Policy Statements)**

### **54.3.1 3.1 Koordination ISMS und Datenschutz**

ISMS und Datenschutz-Management werden koordiniert. CISO und DPO arbeiten eng zusammen und stimmen Maßnahmen ab.

### **54.3.2 3.2 Privacy by Design und by Default**

Datenschutz wird von Anfang an in Systeme und Prozesse integriert (Privacy by Design). Datenschutzfreundliche Voreinstellungen sind Standard (Privacy by Default).

### **54.3.3 3.3 Datenschutz-Folgenabschätzung (DSFA)**

Für risikoreiche Verarbeitungen werden Datenschutz-Folgenabschätzungen durchgeführt. DSFA wird mit ISMS-Risikoanalyse koordiniert.

### **54.3.4 3.4 Betroffenenrechte**

Prozesse zur Erfüllung von Betroffenenrechten sind etabliert: - Auskunftsrecht (Art. 15 DSGVO) - Recht auf Berichtigung (Art. 16 DSGVO) - Recht auf Löschung (Art. 17 DSGVO) - Recht auf Datenübertragbarkeit (Art. 20 DSGVO) - Widerspruchsrecht (Art. 21 DSGVO)

### **54.3.5 3.5 Verzeichnis von Verarbeitungstätigkeiten**

Ein Verzeichnis von Verarbeitungstätigkeiten (VVT) wird geführt und aktuell gehalten. VVT ist mit ISMS-Asset-Inventar abgestimmt.

### **54.3.6 3.6 Auftragsverarbeitung**

Auftragsverarbeiter werden nach DSGVO Art. 28 beauftragt. Auftragsverarbeitungsverträge (AVV) enthalten erforderliche Sicherheitsmaßnahmen.

### **54.3.7 3.7 Datenschutzverletzungen**

Datenschutzverletzungen werden gemäß DSGVO Art. 33/34 behandelt. Meldepflichten an Aufsichtsbehörden und Betroffene werden eingehalten (72-Stunden-Frist).

### **54.3.8 3.8 Internationale Datentransfers**

Internationale Datentransfers erfolgen nur mit angemessenen Garantien (Angemessenheitsbeschluss, Standardvertragsklauseln, BCR).

## **54.4 4. Rollen und Verantwortlichkeiten**

### **54.4.1 RACI-Matrix: Datenschutz Schnittstellen**

Aktivität	CISO	DPO	IT-Betrieb	Business Owner	Legal
Policy-Erstellung	R/A	R/A	C	C	C
DSFA-Durchführung	C	R/A	C	R	C

Aktivität	CISO	DPO	IT-Betrieb	Business Owner	Legal
Betroffenenrechte	I	R/A	C	C	C
VVT-Pflege	C	R/A	C	R	I
AVV-Verhandlung	C	R/A	I	C	R
Data Breach Notification	R/A	R/A	C	C	C
Privacy by Design	R	R/A	R	R	I

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

#### 54.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO) und {{ meta.dpo.name }} (DPO)
- **Data Protection Officer:** {{ meta.dpo.name }}
- **Privacy Officer:** {{ meta.privacy.officer }}
- **Umsetzungsverantwortliche:** IT-Betrieb, Business Owner
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit, Datenschutzaufsicht

### 54.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

#### 54.5.1 Zugehörige Richtlinien

- 0570\_Richtlinie\_Datenschutz\_Anforderungen\_und\_Datenverarbeitung.md - Detaillierte Implementierungsrichtlinie
- 0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md - Data Classification Policy
- 0400\_Policy\_Incident\_Management.md - Incident Management Policy (Data Breaches)
- 0460\_Policy\_Lieferanten\_und\_Cloud\_Sicherheit.md - Supplier Security Policy (AVV)

#### 54.5.2 Zugehörige Standards/Baselinses

- DSFA-Methodik
- Betroffenenrechte-Prozesse
- AVV-Templates
- Data Breach Notification Prozess

#### 54.5.3 Zugehörige Prozesse

- Datenschutz-Folgenabschätzung (DSFA)
- Betroffenenrechte-Prozess
- Data Breach Notification Prozess
- Privacy by Design Review

## 54.6 6. Compliance, Monitoring und Durchsetzung

### 54.6.1 Messgrößen und KPIs

- Anzahl durchgeföhrter DSFAs
- Durchschnittliche Bearbeitungszeit Betroffenenrechte (Ziel: < 30 Tage)
- Anzahl Data Breaches und Meldungen
- VVT-Aktualität (Ziel: quartalsweise Aktualisierung)
- Anzahl AVVs mit aktuellen Sicherheitsmaßnahmen (Ziel: 100%)
- Privacy by Design Review Coverage

### 54.6.2 Nachweise und Evidence

- DSFA-Dokumentation
- Verzeichnis von Verarbeitungstätigkeiten (VVT)
- Betroffenenrechte-Anfragen und Responses
- Auftragsverarbeitungsverträge (AVV)
- Data Breach Notifications
- Privacy by Design Reviews

### 54.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:

- **DSGVO-Verstöße:** Incident Response, Meldung an Aufsichtsbehörde, ggf. Bußgelder - **Nicht gemeldete Data Breaches:** Compliance-Untersuchung, Disziplinarmaßnahmen - **Fehlende DSFAs:** Nachholung, Verarbeitungsstopp - **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen, Bußgelder

## 54.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und DPO genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet

## 54.8 8. Referenzen

### 54.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0570\_Richtlinie\_Datenschutz\_Anforderungen\_und\_Datenverarbeitung.md - Detailed Guideline
- 0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md - Data Classification Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

#### 54.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.5.31 - Legal, statutory, regulatory and contractual requirements
  - ISO/IEC 27001:2022 Annex A.5.32 - Intellectual property rights
  - ISO/IEC 27001:2022 Annex A.5.33 - Protection of records
  - ISO/IEC 27001:2022 Annex A.5.34 - Privacy and protection of PII
  - DSGVO (EU 2016/679) - Datenschutz-Grundverordnung
  - ISO/IEC 27701 - Privacy Information Management System
  - BDSG - Bundesdatenschutzgesetz
- 

**Genehmigt durch:**

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 55

## Richtlinie: Datenschutz-Anforderungen und Datenverarbeitung

**Dokument-ID:** 0570

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0560\_Policy\_Datenschutz\_Schnittstellen.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.34

**Owner:** {{ meta.dpo.name }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 55.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0560\_Policy\_Datenschutz\_Schnittstellen.md und definiert: - DSGVO-Compliance-Anforderungen - Datenverarbeitungsprozesse - Betroffenenrechte und deren Umsetzung

**Geltungsbereich:** Alle personenbezogenen Daten bei **AdminSend GmbH**

### 55.2 2. DSGVO-Grundprinzipien

#### 55.2.1 2.1 Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

**Rechtsgrundlagen (Art. 6 DSGVO):** - Einwilligung (Art. 6 Abs. 1 lit. a) - Vertragserfüllung (Art. 6 Abs. 1 lit. b) - Rechtliche Verpflichtung (Art. 6 Abs. 1 lit. c) - Berechtigtes Interesse (Art. 6 Abs. 1 lit. f)

**Dokumentation:** - Rechtsgrundlage für jede Verarbeitung dokumentieren - Verzeichnis von Verarbeitungstätigkeiten (VVT)

## **55.2.2 2.2 Zweckbindung**

**Prinzip:** - Daten nur für festgelegte, eindeutige Zwecke erheben - Keine Weiterverarbeitung für andere Zwecke (ohne neue Rechtsgrundlage)

## **55.2.3 2.3 Datenminimierung**

**Prinzip:** - Nur notwendige Daten erheben - Regelmäßige Prüfung auf Erforderlichkeit

## **55.2.4 2.4 Richtigkeit**

**Maßnahmen:** - Daten aktuell halten - Fehlerhafte Daten korrigieren - Prozesse für Datenaktualisierung

## **55.2.5 2.5 Speicherbegrenzung**

**Löschkonzept:** - Aufbewahrungsfristen definieren - Automatische Löschung nach Fristablauf - Dokumentation der Löschung

**Details:** Siehe 0590\_Richtlinie\_Records\_Retention\_und\_Sichere\_Loeschung.md

## **55.2.6 2.6 Integrität und Vertraulichkeit**

**Technische Maßnahmen:** - Verschlüsselung - Zugriffskontrolle - Logging und Monitoring

## **55.2.7 2.7 Rechenschaftspflicht**

**Nachweispflicht:** - Dokumentation aller Maßnahmen - Datenschutz-Folgenabschätzung (DSFA) - Verzeichnis von Verarbeitungstätigkeiten (VVT)

# **55.3 3. Verzeichnis von Verarbeitungstätigkeiten (VVT)**

## **55.3.1 3.1 Pflichtangaben (Art. 30 DSGVO)**

**Für jede Verarbeitung:** - Name und Kontaktarten des Verantwortlichen - Zwecke der Verarbeitung - Kategorien betroffener Personen - Kategorien personenbezogener Daten - Kategorien von Empfängern - Drittlandübermittlungen - Löschfristen - Technische und organisatorische Maßnahmen (TOMs)

## **55.3.2 3.2 VVT-Pflege**

**Verantwortlichkeit:** - Datenschutzbeauftragter koordiniert - Fachbereiche liefern Informationen - Jährliche Aktualisierung (mindestens)

**Tool:** {{ meta.dpo.vvt\_tool }}

# **55.4 4. Datenschutz-Folgenabschätzung (DSFA)**

## **55.4.1 4.1 Wann erforderlich?**

**Pflicht bei (Art. 35 DSGVO):** - Systematische umfangreiche Bewertung persönlicher Aspekte (Profiling) - Umfangreiche Verarbeitung besonderer Kategorien (Art. 9) - Systematische umfangreiche

iche Überwachung öffentlicher Bereiche

**Beispiele:** - Neue CRM-Systeme mit Profiling - Videoüberwachung - Biometrische Authentifizierung

#### 55.4.2 4.2 DSFA-Prozess

**Schritte:** 1. Beschreibung der Verarbeitung 2. Bewertung der Notwendigkeit und Verhältnismäßigkeit 3. Risikobewertung für Betroffene 4. Abhilfemaßnahmen 5. Konsultation des Datenschutzbeauftragten 6. Dokumentation

**Bei hohem Risiko:** - Konsultation der Aufsichtsbehörde vor Verarbeitung

### 55.5 5. Betroffenenrechte

#### 55.5.1 5.1 Auskunftsrecht (Art. 15 DSGVO)

**Prozess:** 1. Antrag per E-Mail an {{ meta.dpo.email }} 2. Identitätsprüfung 3. Zusammenstellung der Informationen 4. Antwort innerhalb 1 Monat

**Auszukunftende Informationen:** - Verarbeitungszwecke - Kategorien personenbezogener Daten - Empfänger - Speicherdauer - Betroffenenrechte - Kopie der Daten

#### 55.5.2 5.2 Recht auf Berichtigung (Art. 16 DSGVO)

**Prozess:** 1. Antrag auf Berichtigung 2. Prüfung der Richtigkeit 3. Korrektur innerhalb 1 Monat 4. Benachrichtigung an Empfänger (falls erforderlich)

#### 55.5.3 5.3 Recht auf Löschung (Art. 17 DSGVO)

**Löschgründe:** - Zweck erfüllt - Einwilligung widerrufen - Widerspruch gegen Verarbeitung - Unrechtmäßige Verarbeitung

**Ausnahmen:** - Rechtliche Aufbewahrungspflichten - Geltendmachung von Rechtsansprüchen

#### 55.5.4 5.4 Recht auf Einschränkung (Art. 18 DSGVO)

**Einschränkung statt Löschung:** - Bei Bestreitung der Richtigkeit - Bei unrechtmäßiger Verarbeitung (Betroffener will keine Löschung) - Bei Widerspruch (während Prüfung)

#### 55.5.5 5.5 Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

**Voraussetzungen:** - Verarbeitung auf Einwilligung oder Vertrag - Automatisierte Verarbeitung

**Format:** - Strukturiert, gängig, maschinenlesbar (z.B. CSV, JSON)

#### 55.5.6 5.6 Widerspruchsrecht (Art. 21 DSGVO)

**Bei berechtigtem Interesse:** - Betroffener kann widersprechen - Abwägung erforderlich - Verarbeitung einstellen (außer zwingende Gründe)

**Bei Direktwerbung:** - Widerspruch jederzeit möglich - Verarbeitung sofort einstellen

## 55.6 6. Auftragsverarbeitung

### 55.6.1 6.1 Auftragsverarbeitungsvertrag (AVV)

**Pflicht bei:** - Dienstleister verarbeitet personenbezogene Daten im Auftrag - Cloud-Provider, IT-Dienstleister, etc.

**Pflichtinhalte (Art. 28 DSGVO):** - Gegenstand und Dauer - Art und Zweck der Verarbeitung - Kategorien personenbezogener Daten - Pflichten und Rechte des Verantwortlichen - Technische und organisatorische Maßnahmen (TOMs) - Sub-Auftragsverarbeiter - Unterstützungsplichten

### 55.6.2 6.2 Technische und Organisatorische Maßnahmen (TOMs)

**Kategorien:** - Zutrittskontrolle - Zugangskontrolle - Zugriffskontrolle - Weitergabekontrolle - Eingabekontrolle - Auftragskontrolle - Verfügbarkeitskontrolle - Trennungskontrolle

**Dokumentation:** - TOMs für jede Verarbeitung - Regelmäßige Überprüfung und Anpassung

## 55.7 7. Datenschutzverletzungen (Data Breaches)

### 55.7.1 7.1 Meldepflicht (Art. 33 DSGVO)

**An Aufsichtsbehörde:** - Innerhalb 72 Stunden nach Bekanntwerden - Wenn Risiko für Betroffene

**Ausnahmen:** - Kein Risiko für Betroffene (z.B. verschlüsselte Daten)

### 55.7.2 7.2 Benachrichtigung Betroffener (Art. 34 DSGVO)

**Pflicht bei:** - Hohes Risiko für Betroffene - Ohne unangemessene Verzögerung

**Inhalt:** - Art der Verletzung - Kontaktstelle (Datenschutzbeauftragter) - Wahrscheinliche Folgen - Ergriffene Maßnahmen

### 55.7.3 7.3 Dokumentation

**Verzeichnis von Datenschutzverletzungen:** - Alle Verletzungen dokumentieren (auch nicht meldepflichtige) - Sachverhalt, Auswirkungen, Abhilfemaßnahmen - Nachweis für Aufsichtsbehörde

## 55.8 8. Internationale Datentransfers

### 55.8.1 8.1 Drittlandübermittlung

**Erlaubt bei:** - Angemessenheitsbeschluss der EU-Kommission - Standardvertragsklauseln (SCCs) - Binding Corporate Rules (BCRs) - Einwilligung

### 55.8.2 8.2 Schrems II Compliance

**Transfer Impact Assessment (TIA):** - Rechtslage im Drittland prüfen - Zusätzliche Maßnahmen implementieren (z.B. Verschlüsselung) - Dokumentation

## 55.9 9. Compliance und Audit

### 55.9.1 9.1 Messgrößen (KPIs)

Metrik	Zielwert
Betroffenenanfragen (Antwortzeit)	< 1 Monat
VVT-Aktualität	< 12 Monate
DSFA-Completion (neue Systeme)	100%
Datenschutzverletzungen (Meldung)	< 72 Stunden

### 55.9.2 9.2 Audit-Nachweise

- Verzeichnis von Verarbeitungstätigkeiten (VVT)
- Datenschutz-Folgenabschätzungen (DSFA)
- Auftragsverarbeitungsverträge (AVV)
- Betroffenenanfragen und -antworten
- Verzeichnis von Datenschutzverletzungen

## 55.10 10. Referenzen

### 55.10.1 Interne Dokumente

- 0560\_Policy\_Datenschutz\_Schnittstellen.md
- 0590\_Richtlinie\_Records\_Retention\_und\_Sichere\_Loeschung.md

### 55.10.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.5.34 - Privacy and protection of PII
- DSGVO (EU 2016/679) - Datenschutz-Grundverordnung
- BDSG - Bundesdatenschutzgesetz

---

**Genehmigt durch:** {{ meta.dpo.name }}, Datenschutzbeauftragter

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 56

## Policy: Aufbewahrung und Löschung

**Dokument-ID:** 0580

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.33, A.5.34, A.8.10 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 56.1 1. Zweck

Diese Policy definiert die Anforderungen an Aufbewahrung und Löschung von Informationen und Daten der **AdminSend GmbH**. Sie stellt sicher, dass gesetzliche Aufbewahrungspflichten erfüllt und Datenschutzgrundsätze (Datensparsamkeit, Speicherbegrenzung) eingehalten werden.

### 56.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Daten:** Alle Informationen und Daten (strukturiert und unstrukturiert)
- **Systeme:** Alle IT-Systeme, Datenbanken, Backup-Systeme, Archive
- **Medien:** Digitale und physische Datenträger
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_zulässig).

## **56.3 3. Grundsätze (Policy Statements)**

### **56.3.1 3.1 Aufbewahrungsfristen**

Für alle Informationen werden Aufbewahrungsfristen definiert. Aufbewahrungsfristen basieren auf gesetzlichen, regulatorischen und geschäftlichen Anforderungen.

### **56.3.2 3.2 Retention Schedule**

Ein Retention Schedule (Aufbewahrungsplan) wird erstellt und gepflegt. Der Retention Schedule definiert für jede Informationskategorie: - Aufbewahrungsfrist - Rechtsgrundlage - Löschverfahren - Verantwortliche Rolle

### **56.3.3 3.3 Datensparsamkeit und Speicherbegrenzung**

Daten werden nur so lange aufbewahrt, wie erforderlich (DSGVO Art. 5 Abs. 1 lit. e). Nach Ablauf der Aufbewahrungsfrist werden Daten gelöscht oder anonymisiert.

### **56.3.4 3.4 Sichere Löschung**

Daten werden sicher und unwiederbringlich gelöscht. Löschverfahren stellen sicher, dass Daten nicht wiederhergestellt werden können.

### **56.3.5 3.5 Löschkonzept**

Ein Löschkonzept definiert: - Löschverfahren für verschiedene Datenträger - Löschfristen und Trigger - Verantwortlichkeiten - Nachweisführung

### **56.3.6 3.6 Backup-Aufbewahrung**

Backups unterliegen denselben Aufbewahrungsfristen wie Produktivdaten. Backups werden nach Ablauf der Aufbewahrungsfrist gelöscht.

### **56.3.7 3.7 Legal Hold**

Bei rechtlichen Verfahren oder Untersuchungen können Daten von der Löschung ausgenommen werden (Legal Hold). Legal Hold wird dokumentiert und überwacht.

### **56.3.8 3.8 Physische Datenträger**

Physische Datenträger (Festplatten, USB-Sticks, Papier) werden sicher entsorgt: - Digitale Datenträger: Sichere Löschung oder physische Zerstörung - Papier: Schreddern oder zertifizierte Entsorgung

## **56.4 4. Rollen und Verantwortlichkeiten**

### **56.4.1 RACI-Matrix: Aufbewahrung und Löschung**

Aktivität	CISO	DPO	IT-Betrieb	Business Owner	Records Manager
Policy-Erstellung	R/A	C	C	C	C
Retention Schedule	C	C	C	R	R/A
Löschkonzept	R/A	C	R	C	C
Lösung	I	I	R/A	C	C
Durchführung					
Legal Hold	C	C	I	C	R/A
Backup-Lösung	C	I	R/A	I	C
Physische Entsorgung	C	I	R/A	I	C

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

#### 56.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **Records Manager:** {{ meta.records.manager }}
- **Data Protection Officer:** {{ meta.dpo.name }}
- **Umsetzungsverantwortliche:** IT-Betrieb, Business Owner
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit, Legal

### 56.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

#### 56.5.1 Zugehörige Richtlinien

- **0590\_Richtlinie\_Records\_Retention\_und\_Sichere\_Loeschung.md** - Detaillierte Implementierungsrichtlinie
- **0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md** - Data Classification Policy
- **0560\_Policy\_Datenschutz\_Schnittstellen.md** - Privacy Policy
- **0420\_Policy\_Backup\_und\_Wiederherstellung.md** - Backup Policy

#### 56.5.2 Zugehörige Standards/Baselinses

- Retention Schedule (Aufbewahrungsplan)
- Löschkonzept
- Sichere Löscherfahren (NIST SP 800-88, BSI TL-03423)
- Legal Hold Prozess

#### 56.5.3 Zugehörige Prozesse

- Retention Management Prozess

- Löschprozess (automatisiert und manuell)
- Legal Hold Prozess
- Physische Entsorgung Prozess

## 56.6 6. Compliance, Monitoring und Durchsetzung

### 56.6.1 Messgrößen und KPIs

- Retention Schedule Coverage (Ziel: 100% aller Informationskategorien)
- Anzahl durchgeföhrter Löschungen (geplant vs. durchgeführt)
- Durchschnittliche Zeit bis zur Löschung nach Fristablauf (Ziel: < 30 Tage)
- Anzahl Legal Holds und Dauer
- Backup-Löschung Compliance (Ziel: 100%)
- Anzahl sicher entsorgter physischer Datenträger

### 56.6.2 Nachweise und Evidence

- Retention Schedule
- Löschprotokolle und Nachweise
- Legal Hold Dokumentation
- Backup-Löschprotokolle
- Entsorgungsnachweise (Zertifikate)
- Audit Logs für Löschungen

### 56.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt: - **Nicht gelöschte Daten:** Nachholung, Compliance-Untersuchung - **Fehlende Retention Schedule:** Erstellung, Risikobewertung - **Unsichere Löschung:** Incident Response, Risikobewertung - **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen, Bußgelder

## 56.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und DPO genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet

## 56.8 8. Referenzen

### 56.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0590\_Richtlinie\_Records\_Retention\_und\_Sichere\_Loeschung.md - Detailed Guideline
- 0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md - Data Classification Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

## 56.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.5.33 - Protection of records
  - ISO/IEC 27001:2022 Annex A.5.34 - Privacy and protection of PII
  - ISO/IEC 27001:2022 Annex A.8.10 - Information deletion
  - DSGVO Art. 5 Abs. 1 lit. e - Speicherbegrenzung
  - DSGVO Art. 17 - Recht auf Löschung
  - NIST SP 800-88 - Guidelines for Media Sanitization
  - BSI TL-03423 - Leitfaden zur Löschung und Vernichtung
- 

**Genehmigt durch:**

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 57

## Richtlinie: Records Retention und Sichere Löschung

**Dokument-ID:** 0590

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0580\_Policy\_Aufbewahrung\_und\_Loeschung.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.33

**Owner:** {{ meta.compliance.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 57.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0580\_Policy\_Aufbewahrung\_und\_Loeschung.md und definiert: - Aufbewahrungsfristen für verschiedene Datentypen - Sichere Löschverfahren - Records Management Prozesse

**Geltungsbereich:** Alle Daten und Dokumente bei **AdminSend GmbH**

### 57.2 2. Aufbewahrungsfristen

#### 57.2.1 2.1 Geschäftsdokumente

Dokumenttyp	Aufbewahrungsfrist	Rechtsgrundlage
Jahresabschlüsse	10 Jahre	HGB §257
Buchungsbelege	10 Jahre	HGB §257
Rechnungen	10 Jahre	HGB §257, AO §147
Verträge	10 Jahre nach Ende	HGB §257
Geschäftskorrespondenz	6 Jahre	HGB §257
Angebote	6 Jahre	HGB §257

## 57.2.2 2.2 Personaldokumente

Dokumenttyp	Aufbewahrungsfrist	Rechtsgrundlage
Personalakten	10 Jahre nach Austritt	DSGVO Art. 17
Lohnabrechnungen	10 Jahre	AO §147
Arbeitszeugnisse	3 Jahre	BGB §195
Bewerbungsunterlagen (abgelehnt)	6 Monate	AGG §15
Zeiterfassungsdaten	2 Jahre	ArbZG §16

## 57.2.3 2.3 IT-Daten

Datentyp	Aufbewahrungsfrist	Begründung
E-Mails (geschäftlich)	{{ meta.retention.email_years }} Jahre	Geschäftskorrespondenz
Logs (Security)	{{ meta.retention.log_years }} Jahre	Forensik, Compliance
Logs (System)	1 Jahr	Troubleshooting
Backups	Gemäß Backup-Policy	Wiederherstellung
Audit-Trails	{{ meta.retention.audit_years }} Jahre	Compliance

## 57.2.4 2.4 Kundendaten

Datentyp	Aufbewahrungsfrist	Rechtsgrundlage
Kundenstammdaten	Bis Vertragsende + 3 Jahre	Verjährung
Bestelldaten	10 Jahre	HGB §257
Zahlungsdaten	10 Jahre	AO §147
Kommunikation	6 Jahre	HGB §257

## 57.3 3. Retention-Management

### 57.3.1 3.1 Retention-Policies

**Automatisierung:** - Retention-Labels in Microsoft 365 - Lifecycle-Policies in Cloud-Storage - Automatische Löschung nach Fristablauf

**Manuelle Prozesse:** - Für physische Dokumente - Für Legacy-Systeme

### 57.3.2 3.2 Legal Hold

**Bei rechtlichen Verfahren:** - Aussetzung der Löschung - Preservation Order - Dokumentation des Legal Hold - Aufhebung nach Verfahrensende

### 57.3.3 3.3 Retention-Register

**Dokumentation:** - Datentyp, Aufbewahrungsfrist, Rechtsgrundlage - Speicherort, Verantwortlicher - Löschdatum - Regelmäßige Reviews (jährlich)

## 57.4 4. Sichere Löschung

### 57.4.1 4.1 Digitale Daten

Methoden nach DIN 66399:

Datenträger	Methode	Standard
HDD	Software-Lösung (3-Pass) oder Degaussing	DIN 66399 H-3/H-4
SSD	Secure Erase (ATA) oder Kryptographische Lösung	DIN 66399 H-3
Cloud-Daten	Logische Lösung + Bestätigung	Provider-abhängig
Backups	Kryptographische Lösung (Schlüssel vernichten)	DIN 66399 H-4

**Tools:** - DBAN, Blancco (Software-Lösung) - Degausser (Magnetische Lösung) - Shredder (Physische Zerstörung)

### 57.4.2 4.2 Physische Dokumente

Methoden nach DIN 66399:

Schutzstufe	Partikelgröße	Anwendung
P-3	320 mm <sup>2</sup>	Interne Dokumente
P-4	160 mm <sup>2</sup>	Vertrauliche Dokumente
P-5	30 mm <sup>2</sup>	Streng vertrauliche Dokumente

**Prozess:** - Shredder in Büros (P-3) - Zertifizierte Entsorgungspartner (P-4, P-5) - Entsorgungsnachweis

### 57.4.3 4.3 Löschprotokoll

**Dokumentation:** - Datum der Lösung - Gelöschte Daten/Dokumente - Löschnmethode - Durchführende Person - Bestätigung der Lösung

**Retention:** {{ meta.retention.deletion\_log\_years }} Jahre

## 57.5 5. E-Mail-Archivierung

### 57.5.1 5.1 Archivierungspflicht

**Geschäftliche E-Mails:** - Automatische Archivierung - Unveränderbarkeit (WORM) - Aufbewahrung: {{ meta.retention.email\_years }} Jahre

**Private E-Mails:** - Keine Archivierung - Kennzeichnung durch Nutzer (Betreff: [PRIVAT])

## 57.5.2 5.2 Archivierungssystem

**System:** {{ meta.email.archive\_system }}

**Funktionen:** - Automatische Archivierung - Volltextsuche - eDiscovery - Legal Hold

## 57.5.3 5.3 Zugriff auf Archiv

**Berechtigungen:** - Nutzer: Eigene E-Mails - Vorgesetzte: Bei berechtigtem Interesse (mit Genehmigung) - Legal/Compliance: Für Audits und Ermittlungen - IT-Admins: Nur für technische Administration

# 57.6 6. Datenminimierung

## 57.6.1 6.1 Privacy by Design

**Prinzipien:** - Nur notwendige Daten erheben - Kürzeste Aufbewahrungsfrist wählen - Automatische Löschung implementieren

## 57.6.2 6.2 Regelmäßige Reviews

**Quartalsweise:** - Ungenutzte Daten identifizieren - Löschung prüfen - Retention-Policies anpassen

# 57.7 7. Cloud-Daten-Löschung

## 57.7.1 7.1 SaaS-Anwendungen

**Prozess:** 1. Logische Löschung in Anwendung 2. Warten auf Retention-Period (Provider-abhängig)  
3. Bestätigung der endgültigen Löschung anfordern 4. Dokumentation

## 57.7.2 7.2 IaaS/PaaS

**Prozess:** 1. Daten löschen 2. Volumes/Disks löschen 3. Snapshots löschen 4. Kryptographische Schlüssel vernichten 5. Bestätigung der Löschung

# 57.8 8. Compliance und Audit

## 57.8.1 8.1 Messgrößen (KPIs)

Metrik	Zielwert
Automatische Löschung (nach Frist)	100%
Löschprotokoll-Vollständigkeit	100%
Retention-Policy-Compliance	> 95%
Entsorgungsnachweise	100%

## 57.8.2 8.2 Audit-Nachweise

- Retention-Register
- Löschprotokolle

- Entsorgungsnachweise
- E-Mail-Archivierungs-Berichte

## 57.9 9. Referenzen

### 57.9.1 Interne Dokumente

- 0580\_Policy\_Aufbewahrung\_und\_Loeschung.md
- 0570\_Richtlinie\_Datenschutz\_Anforderungen\_und\_Datenverarbeitung.md

### 57.9.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.5.33 - Protection of records
- DIN 66399 - Vernichtung von Datenträgern
- HGB §257 - Aufbewahrung von Unterlagen
- AO §147 - Ordnungsvorschriften für die Aufbewahrung von Unterlagen

---

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 58

## Policy: Netzwerksicherheit

**Dokument-ID:** 0600

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.8.20-A.8.23 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 58.1 1. Zweck

Diese Policy definiert die Anforderungen an die Netzwerksicherheit der **AdminSend GmbH**. Sie stellt sicher, dass Netzwerke angemessen gesichert, segmentiert und überwacht werden, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu schützen.

### 58.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Netzwerke:** Alle internen und externen Netzwerke, LAN, WLAN, WAN, VPN
- **Systeme:** Firewalls, Router, Switches, Load Balancer, IDS/IPS
- **Verbindungen:** Alle Netzwerkverbindungen (intern, extern, Partner, Cloud)
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_zulässig).

## **58.3 3. Grundsätze (Policy Statements)**

### **58.3.1 3.1 Netzwerksegmentierung**

Netzwerke werden nach Schutzbedarf und Funktion segmentiert. Segmentierung erfolgt durch Firewalls, VLANs und Zonen (z.B. DMZ, Produktionsnetz, Verwaltungsnetz).

### **58.3.2 3.2 Defense in Depth**

Netzwerksicherheit folgt dem Defense-in-Depth-Prinzip. Mehrere Sicherheitsschichten schützen vor Angriffen (Perimeter, Segmentierung, Host-basiert).

### **58.3.3 3.3 Least Privilege Network Access**

Netzwerkzugriffe folgen dem Least-Privilege-Prinzip. Nur erforderliche Verbindungen sind erlaubt (Default Deny, Whitelist-Ansatz).

### **58.3.4 3.4 Firewall-Management**

Firewalls schützen Netzwerkgrenzen. Firewall-Regeln werden dokumentiert, regelmäßig überprüft und nach Change-Management-Prozess geändert.

### **58.3.5 3.5 Network Access Control (NAC)**

Zugriffe auf Netzwerke werden kontrolliert. NAC stellt sicher, dass nur autorisierte und konforme Geräte Zugriff erhalten.

### **58.3.6 3.6 Intrusion Detection/Prevention (IDS/IPS)**

Netzwerke werden auf Angriffe überwacht. IDS/IPS-Systeme erkennen und blockieren verdächtige Aktivitäten.

### **58.3.7 3.7 VPN und Remote Access**

Remote-Zugriffe erfolgen über sichere VPN-Verbindungen. VPN-Verbindungen sind verschlüsselt und authentifiziert (MFA).

### **58.3.8 3.8 Wireless Security**

WLAN-Netzwerke sind gesichert (WPA3, 802.1X). Gast-WLANs sind vom Produktionsnetz getrennt.

### **58.3.9 3.9 Network Monitoring und Logging**

Netzwerkaktivitäten werden überwacht und protokolliert. Logs werden zentral gesammelt und analysiert (SIEM).

## **58.4 4. Rollen und Verantwortlichkeiten**

### **58.4.1 RACI-Matrix: Netzwerksicherheit**

Aktivität	CISO	Network Security	IT-Betrieb	SOC	Network Admin
Policy-Erstellung	R/A	R	C	C	C
Netzwerksegmentierung	R/A		R	C	R
Firewall-Management	C	R/A	R	C	R
NAC-Implementierung	C	R/A	R	C	R
IDS/IPS-Betrieb	C	R	C	R/A	C
VPN-Management	C	R/A	R	C	R
WLAN-Security	C	R/A	R	C	R
Network Monitoring	C	R	C	R/A	C

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

#### 58.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **Network Security Manager:** {{ meta.network.security\_manager }}
- **Network Administrator:** {{ meta.network.admin }}
- **SOC Manager:** {{ meta.soc.manager }}
- **Umsetzungsverantwortliche:** IT-Betrieb, Network Team
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit, SOC

### 58.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

#### 58.5.1 Zugehörige Richtlinien

- **0610\_Richtlinie\_Segmentierung\_Firewalling\_und\_Network\_Access\_Control.md**  
- Detaillierte Implementierungsrichtlinie
- **0220\_Policy\_Zugriffssteuerung\_und\_Identitätsmanagement.md** - Access Control Policy
- **0320\_PolicyLogging\_und\_Monitoring.md** - Logging and Monitoring Policy
- **0500\_Policy\_Mobile\_Device\_und\_Remote\_Work.md** - Remote Work Policy

#### 58.5.2 Zugehörige Standards/Baselinses

- Netzwerksegmentierungskonzept
- Firewall-Regelwerk
- NAC-Konfiguration
- IDS/IPS-Signaturen und Regeln

- VPN-Konfiguration
- WLAN-Security-Baseline

### 58.5.3 Zugehörige Prozesse

- Firewall Change Management
- NAC Onboarding/Offboarding
- IDS/IPS Alert Response
- VPN Access Request
- Network Security Monitoring

## 58.6 6. Compliance, Monitoring und Durchsetzung

### 58.6.1 Messgrößen und KPIs

- Netzwerksegmentierung Coverage (Ziel: 100% kritischer Systeme)
- Firewall-Regel-Review-Frequenz (Ziel: quartalsweise)
- NAC Coverage (Ziel: 100% Produktionsnetz)
- IDS/IPS Alert Response Time (Ziel: < 15 Minuten für kritische Alerts)
- VPN-Verfügbarkeit (Ziel: 99.5%)
- WLAN-Security-Compliance (Ziel: 100% WPA3)
- Anzahl blockierter Angriffe (IDS/IPS)

### 58.6.2 Nachweise und Evidence

- Netzwerkdiagramme und Segmentierungskonzept
- Firewall-Regelwerk und Change-Logs
- NAC-Konfiguration und Device-Inventory
- IDS/IPS-Logs und Alert-Reports
- VPN-Logs und Access-Logs
- WLAN-Konfiguration und Security-Scans
- Network Monitoring Dashboards

### 58.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:

- **Nicht autorisierte Firewall-Änderungen:** Incident Response, Rollback, Disziplinarmaßnahmen
- **Fehlende Segmentierung:** Nachholung, Risikobewertung
- **Unsichere WLAN-Konfiguration:** Sofortige Korrektur, Incident Response
- **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen, Zugriffsentzug

## 58.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und Network Security Manager genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert

- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet

## 58.8 8. Referenzen

### 58.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0610\_Richtlinie\_Segmentierung\_Firewalling\_und\_Network\_Access\_Control.md - Detailed Guideline
- 0220\_Policy\_Zugriffssteuerung\_und\_Identitätsmanagement.md - Access Control Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

### 58.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.8.20 - Networks security
  - ISO/IEC 27001:2022 Annex A.8.21 - Security of network services
  - ISO/IEC 27001:2022 Annex A.8.22 - Segregation of networks
  - ISO/IEC 27001:2022 Annex A.8.23 - Web filtering
  - NIST SP 800-41 - Guidelines on Firewalls and Firewall Policy
  - NIST SP 800-97 - Establishing Wireless Robust Security Networks
  - BSI IT-Grundschutz - NET.1.1, NET.1.2, NET.3.2
- 

**Genehmigt durch:**

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 59

## Richtlinie: Segmentierung, Firewalling und Network Access Control

**Dokument-ID:** 0610

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0600\_Policy\_Netzwerksicherheit.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.8.20, A.8.21, A.8.22

**Owner:** {{ meta.network.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Vertraulich

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 59.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0600\_Policy\_Netzwerksicherheit.md und definiert: - Netzwerk-Segmentierung und Zonen-Modell - Firewall-Regeln und -Management - Network Access Control (NAC)

**Geltungsbereich:** Alle Netzwerke bei AdminSend GmbH

### 59.2 2. Netzwerk-Segmentierung

#### 59.2.1 2.1 Zonen-Modell

**Zone 1: Internet (Untrusted)** - Öffentliches Internet - Keine Vertrauensstellung

**Zone 2: DMZ (Demilitarized Zone)** - Internet-facing Services (Web-Server, E-Mail-Gateway) - Eingeschränkter Zugriff auf interne Ressourcen

**Zone 3: Corporate Network** - Interne Büro-Netzwerke - Workstations, Drucker - Standard-Sicherheitskontrollen

**Zone 4: Server Network** - Interne Server (File-Server, Application-Server) - Erhöhte Sicherheitskontrollen

**Zone 5: Management Network** - Management-Interfaces (IPMI, iLO, iDRAC) - Out-of-Band-Management - Höchste Sicherheitskontrollen

**Zone 6: Production Network** - Kritische Produktionssysteme - Datenbanken, ERP - Höchste Sicherheitskontrollen

## 59.2.2 2.2 VLAN-Segmentierung

**VLAN-Schema:** - VLAN 10: Management - VLAN 20: Server - VLAN 30: Workstations - VLAN 40: Guest/BYOD - VLAN 50: IoT/OT - VLAN 60: DMZ

**Inter-VLAN-Routing:** - Über Firewall (nicht Layer-3-Switch) - Explizite Firewall-Regeln erforderlich

## 59.2.3 2.3 Micro-Segmentation

**Für kritische Systeme:** - Segmentierung auf Workload-Ebene - Software-Defined Networking (SDN) - Zero Trust Network Access (ZTNA)

# 59.3 3. Firewall-Management

## 59.3.1 3.1 Firewall-Architektur

**Perimeter-Firewall:** - Internet DMZ - Internet Corporate Network - Hochverfügbarkeit (Active/Active oder Active/Passive)

**Internal Firewalls:** - Zwischen Zonen - Micro-Segmentation

**Firewall-Plattform:** {{ meta.network.firewall }}

## 59.3.2 3.2 Firewall-Regeln

**Default Deny:** - Alle Verbindungen standardmäßig blockiert - Nur explizit erlaubte Verbindungen

**Regel-Struktur:** - Quelle (IP/Netzwerk) - Ziel (IP/Netzwerk) - Service (Port/Protokoll) - Aktion (Allow/Deny) - Logging (Enabled) - Begründung (Business Justification)

**Regel-Reihenfolge:** 1. Deny-Regeln (spezifisch) 2. Allow-Regeln (spezifisch zu allgemein) 3. Default Deny (implizit)

## 59.3.3 3.3 Firewall-Change-Prozess

**Antrag:** - Change Request über Ticketsystem - Begründung (Business Justification) - Quell- und Ziel-IP/Port - Zeitliche Befristung (wo möglich)

**Genehmigung:** - IT-Security: Verpflichtend - Network-Team: Technische Umsetzbarkeit - Application-Owner: Business Justification

**Implementation:** - Testing in Dev/Test (wo möglich) - Implementation in Wartungsfenster - Verification - Dokumentation

**Details:** Siehe 0370\_Richtlinie\_Change\_Management

#### 59.3.4 3.4 Firewall-Review

**Regelmäßige Reviews:** - Quartalsweise: Alle Firewall-Regeln reviewen - Ungenutzte Regeln identifizieren - Temporäre Regeln verlängern oder löschen - Dokumentation aktualisieren

### 59.4 4. Network Access Control (NAC)

#### 59.4.1 4.1 NAC-System

**Plattform:** {{ meta.network.nac\_solution }} (z.B. Cisco ISE, Aruba ClearPass)

**Funktionen:** - 802.1X Authentifizierung - MAC-Address-Authentication (MAB) - Guest-Access - Posture-Assessment

#### 59.4.2 4.2 802.1X Authentifizierung

**Für Workstations:** - Computer-Authentifizierung (Machine Auth) - Benutzer-Authentifizierung (User Auth) - Zertifikat-basiert oder EAP-TLS

**Für Server:** - Zertifikat-basierte Authentifizierung - Dedizierte VLANs

#### 59.4.3 4.3 Posture-Assessment

**Compliance-Checks:** - Antivirus aktiv und aktuell? - Firewall aktiviert? - OS-Patches aktuell? - Disk-Verschlüsselung aktiviert?

**Bei Non-Compliance:** - Quarantäne-VLAN - Eingeschränkter Zugriff (nur Patch-Server) - Benachrichtigung an Nutzer

#### 59.4.4 4.4 Guest-Access

**Guest-VLAN:** - Isoliert von Corporate Network - Nur Internet-Zugriff - Captive Portal für Registrierung

**Prozess:** 1. Gast registriert sich (Self-Service oder Sponsor) 2. Credentials per SMS/E-Mail 3. Zeitlich befristeter Zugang (max. 24 Stunden) 4. Automatische Deaktivierung

### 59.5 5. Intrusion Detection/Prevention (IDS/IPS)

#### 59.5.1 5.1 IDS/IPS-Platzierung

**Perimeter:** - Vor Firewall (IDS) - Hinter Firewall (IPS)

**Intern:** - Zwischen kritischen Zonen - IPS-Modus

**IDS/IPS-System:** {{ meta.security.ids\_ips }}

#### 59.5.2 5.2 Signaturen und Policies

**Signature-Updates:** - Automatisch, täglich - Kritische Signaturen: Sofort

**IPS-Policies:** - Balanced (Standard) - Connectivity (weniger aggressiv) - Security (aggressiver)

### **59.5.3 5.3 Alerting**

**SIEM-Integration:** - Alle IDS/IPS-Alerts zu SIEM - Korrelation mit anderen Events - Automatische Response (bei kritischen Alerts)

## **59.6 6. VPN und Remote Access**

### **59.6.1 6.1 VPN-Typen**

**Site-to-Site VPN:** - Zwischen Standorten - IPsec - Always-On

**Remote Access VPN:** - Für Remote-Mitarbeiter - SSL-VPN oder IPsec - MFA verpflichtend

**Details:** Siehe 0510\_Richtlinie\_MDM\_BringYourOwnDevice\_und\_Remote\_Access.md

### **59.6.2 6.2 VPN-Segmentierung**

**VPN-Nutzer in separatem VLAN:** - Nicht direkt im Corporate Network - Firewall-Regeln für Zugriff - Posture-Assessment vor Zugriff

## **59.7 7. Wireless Security**

### **59.7.1 7.1 WLAN-Segmentierung**

**Corporate WLAN:** - 802.1X Authentifizierung - WPA3-Enterprise - Zugriff auf Corporate Resources

**Guest WLAN:** - Captive Portal - WPA2/WPA3-Personal - Nur Internet-Zugriff

**IoT WLAN:** - Separates VLAN - MAC-Address-Whitelist - Eingeschränkter Zugriff

### **59.7.2 7.2 WLAN-Security**

**Verschlüsselung:** - WPA3-Enterprise (Corporate) - WPA2/WPA3-Personal (Guest) - Kein WEP, WPA

**Rogue AP Detection:** - Automatische Scans - Alerts bei unautorisierten APs

## **59.8 8. Network Monitoring**

### **59.8.1 8.1 Flow-Monitoring**

**NetFlow/sFlow:** - Sammlung von Flow-Daten - Analyse von Traffic-Mustern - Anomalie-Erkennung

**Tools:** {{ meta.network.flow\_tool }}

### **59.8.2 8.2 Packet Capture**

**Für Forensik:** - Packet-Capture an kritischen Punkten - Retention: 7 Tage - Zugriff nur für Security-Team

## 59.9 9. Compliance und Audit

### 59.9.1 9.1 Messgrößen (KPIs)

Metrik	Zielwert
Firewall-Regel-Review-Completion	100% quartalsweise
Ungenutzte Firewall-Regeln	< 10%
NAC-Compliance-Rate	> 95%
IPS-False-Positive-Rate	< 5%

### 59.9.2 9.2 Audit-Nachweise

- Firewall-Konfigurationen
- Firewall-Change-Logs
- NAC-Compliance-Reports
- IDS/IPS-Alerts und -Responses

## 59.10 10. Referenzen

### 59.10.1 Interne Dokumente

- 0600\_Policy\_Netzwerksicherheit.md
- 0370\_Richtlinie\_Change\_Management\_mit\_Sicherheitsfreigaben.md

### 59.10.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.8.20 - Networks security
- ISO/IEC 27001:2022 Annex A.8.21 - Security of network services
- ISO/IEC 27001:2022 Annex A.8.22 - Segregation of networks
- NIST SP 800-41 - Guidelines on Firewalls and Firewall Policy

---

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 60

## Policy: Endpoint Security

**Dokument-ID:** 0620

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.8.1-A.8.3, A.6.7 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 60.1 1. Zweck

Diese Policy definiert die Anforderungen an die Endpoint Security der **AdminSend GmbH**. Sie stellt sicher, dass alle Endgeräte (Workstations, Laptops, mobile Geräte) angemessen gesichert sind und vor Bedrohungen geschützt werden.

### 60.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Geräte:** Alle Endgeräte (Workstations, Laptops, Tablets, Smartphones)
- **Betriebssysteme:** Windows, macOS, Linux, iOS, Android
- **Eigentum:** Unternehmenseigene und BYOD-Geräte (mit Unternehmenszugriff)
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte, Remote Work

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_) zulässig.

## **60.3 3. Grundsätze (Policy Statements)**

### **60.3.1 3.1 Endpoint Protection Platform (EPP)**

Alle Endgeräte sind mit Endpoint Protection ausgestattet. EPP umfasst Antivirus, Anti-Malware, Host-Firewall und Application Control.

### **60.3.2 3.2 Endpoint Detection and Response (EDR)**

Kritische Endgeräte sind mit EDR-Lösung ausgestattet. EDR ermöglicht erweiterte Bedrohungserkennung, Incident Response und Forensik.

### **60.3.3 3.3 Device Compliance**

Endgeräte müssen Compliance-Anforderungen erfüllen: - Aktuelle Betriebssystem-Version - Aktuelle Security-Patches - EPP/EDR installiert und aktiv - Disk Encryption aktiviert - Screen Lock konfiguriert

### **60.3.4 3.4 Disk Encryption**

Alle Endgeräte mit Unternehmensdaten sind verschlüsselt (Full Disk Encryption). Verschlüsselung schützt vor Datenverlust bei Diebstahl oder Verlust.

### **60.3.5 3.5 Host-based Firewall**

Alle Endgeräte haben eine aktivierte Host-Firewall. Firewall-Regeln folgen dem Least-Privilege-Prinzip.

### **60.3.6 3.6 Application Control**

Nicht autorisierte Anwendungen werden blockiert (Application Whitelisting oder Blacklisting). Application Control reduziert Malware-Risiko.

### **60.3.7 3.7 Patch Management**

Endgeräte werden regelmäßig gepatcht. Security-Patches werden zeitnah installiert (siehe 0340\_Policy\_Vulnerability\_und\_Patch\_Management.md).

### **60.3.8 3.8 Remote Wipe**

Verlorene oder gestohlene Geräte können remote gelöscht werden. Remote Wipe schützt vor Datenverlust.

### **60.3.9 3.9 BYOD (Bring Your Own Device)**

BYOD-Geräte mit Unternehmenszugriff müssen Mindest-Sicherheitsanforderungen erfüllen. BYOD wird über MDM/MAM verwaltet (siehe 0500\_Policy\_Mobile\_Device\_und\_Remote\_Work.md).

## 60.4 4. Rollen und Verantwortlichkeiten

### 60.4.1 RACI-Matrix: Endpoint Security

Aktivität	CISO	Endpoint Security	IT-Betrieb	SOC	End User
Policy-Erstellung	R/A	R	C	C	I
EPP/EDR-Deployment	C	R/A	R	C	I
Device Compliance	C	R/A	R	C	R
Disk Encryption	C	R/A	R	I	C
Patch Management	C	R	R/A	I	C
Remote Wipe	C	R/A	C	C	I
BYOD-Management	C	R/A	R	I	R
Incident Response	C	R	C	R/A	I

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

### 60.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **Endpoint Security Manager:** {{ meta.endpoint.security\_manager }}
- **IT Operations Manager:** {{ meta.it.operations\_manager }}
- **SOC Manager:** {{ meta.soc.manager }}
- **Umsetzungsverantwortliche:** IT-Betrieb, End Users
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit, SOC

## 60.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

### 60.5.1 Zugehörige Richtlinien

- **0630\_Richtlinie\_EDR\_AV\_Host\_Firewall\_und\_Device\_Compliance.md** - Detaillierte Implementierungsrichtlinie
- **0500\_Policy\_Mobile\_Device\_und\_Remote\_Work.md** - Mobile Device Policy
- **0340\_Policy\_Vulnerability\_und\_Patch\_Management.md** - Patch Management Policy
- **0260\_Policy\_Kryptografie\_und\_Schluesselmanagement.md** - Encryption Policy

### 60.5.2 Zugehörige Standards/Baselinses

- Endpoint Security Baseline (Windows, macOS, Linux)
- EPP/EDR-Konfiguration
- Device Compliance Requirements
- Disk Encryption Standards
- Application Whitelist/Blacklist

### 60.5.3 Zugehörige Prozesse

- Endpoint Onboarding/Offboarding
- Device Compliance Monitoring
- EPP/EDR Alert Response
- Remote Wipe Prozess
- BYOD Enrollment

## 60.6 6. Compliance, Monitoring und Durchsetzung

### 60.6.1 Messgrößen und KPIs

- EPP/EDR Coverage (Ziel: 100% aller Endgeräte)
- Device Compliance Rate (Ziel: >95%)
- Disk Encryption Coverage (Ziel: 100%)
- Patch Compliance (Ziel: >95% innerhalb SLA)
- EPP/EDR Detection Rate
- Durchschnittliche Incident Response Time (Ziel: < 30 Minuten)
- Anzahl Remote Wipes

### 60.6.2 Nachweise und Evidence

- Endpoint Inventory
- EPP/EDR-Deployment-Status
- Device Compliance Reports
- Disk Encryption Status
- Patch Compliance Reports
- EPP/EDR-Logs und Alerts
- Remote Wipe Logs

### 60.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:

- **Non-compliant Devices:** Netzwerzugriff blockiert bis Compliance hergestellt
- **Deaktivierte EPP/EDR:** Sofortige Reaktivierung, Incident Response
- **Fehlende Disk Encryption:** Nachholung, Zugriffsbeschränkung
- **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen, Gerätenutzung untersagt

## 60.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und Endpoint Security Manager genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet

## 60.8 8. Referenzen

### 60.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0630\_Richtlinie\_EDR\_AV\_Host\_Firewall\_und\_Device\_Compliance.md - Detailed Guide-line
- 0500\_Policy\_Mobile\_Device\_und\_Remote\_Work.md - Mobile Device Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

### 60.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.8.1 - User endpoint devices
- ISO/IEC 27001:2022 Annex A.8.2 - Privileged access rights
- ISO/IEC 27001:2022 Annex A.8.3 - Information access restriction
- ISO/IEC 27001:2022 Annex A.6.7 - Remote working
- NIST SP 800-124 - Guidelines for Managing the Security of Mobile Devices
- NIST SP 800-171 - Protecting Controlled Unclassified Information
- CIS Controls v8 - Control 4 (Secure Configuration of Enterprise Assets)

---

#### Genehmigt durch:

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

Nächster Review: {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 61

## Richtlinie: EDR, Antivirus, Host-Firewall und Device Compliance

**Dokument-ID:** 0630

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0620\_Policy\_Endpoint\_Security.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.8.7

**Owner:** {{ meta.it\_operations.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 61.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0620\_Policy\_Endpoint\_Security.md und definiert: - Endpoint Detection and Response (EDR) Anforderungen - Antivirus-Konfiguration und -Management - Host-Firewall-Policies - Device-Compliance-Anforderungen

**Geltungsbereich:** Alle Endpoints bei AdminSend GmbH

### 61.2 2. Endpoint Detection and Response (EDR)

#### 61.2.1 2.1 EDR-System

**Plattform:** {{ meta.security.edr\_solution }} (z.B. CrowdStrike, SentinelOne, Microsoft Defender for Endpoint)

**Funktionen:** - Real-time Threat Detection - Behavioral Analysis - Automated Response - Forensic Capabilities - Threat Hunting

## 61.2.2 2.2 EDR-Deployment

**Pflicht-Installation:** - Alle Workstations (Windows, macOS, Linux) - Alle Server - Keine Ausnahmen (außer über Ausnahmenprozess)

**Deployment-Methoden:** - Group Policy (Windows) - MDM (macOS, Mobile) - Configuration Management (Linux)

## 61.2.3 2.3 EDR-Policies

**Detection-Modi:** - **Prevent:** Automatische Blockierung (Standard) - **Detect:** Nur Alerting (für Legacy-Systeme)

**Behavioral Policies:** - Ransomware-Protection - Credential-Theft-Protection - Exploit-Protection - Script-Control (PowerShell, CMD)

## 61.2.4 2.4 EDR-Response

**Automatische Aktionen:** - Malware-Quarantäne - Prozess-Terminierung - Netzwerk-Isolation (bei kritischen Threats)

**Manuelle Aktionen:** - Remote Shell für Forensik - File Retrieval - Memory Dump

## 61.2.5 2.5 Tamper Protection

**Schutz vor Deaktivierung:** - EDR-Agent kann nicht deaktiviert werden (ohne Admin-Passwort) - Uninstall-Passwort erforderlich - Alerts bei Tamper-Versuchen

## 61.3 3. Antivirus (AV)

### 61.3.1 3.1 AV-System

**Plattform:** {{ meta.security.av\_solution }} (oft integriert in EDR)

**Scan-Typen:** - Real-time Scanning (On-Access) - Scheduled Full Scans (wöchentlich) - Quick Scans (täglich)

### 61.3.2 3.2 AV-Konfiguration

**Scan-Einstellungen:** - Alle Dateitypen scannen - Archive scannen - E-Mail-Anhänge scannen - Removable Media scannen

**Exclusions:** - Nur nach Genehmigung durch IT-Security - Dokumentation erforderlich - Regelmäßiger Review (quartalsweise)

### 61.3.3 3.3 Signature-Updates

**Automatische Updates:** - Mehrmals täglich - Über interne Update-Server (WSUS, etc.) - Fall-back auf Cloud-Updates

**Monitoring:** - Alerts bei veralteten Signaturen (> 7 Tage)

### **61.3.4 3.4 Malware-Handling**

**Bei Malware-Detektion:** 1. Automatische Quarantäne 2. Alert an Security-Team 3. Incident-Ticket erstellen 4. Forensische Analyse (bei Bedarf) 5. Remediation 6. Lessons Learned

## **61.4 4. Host-Firewall**

### **61.4.1 4.1 Windows Firewall**

**Konfiguration via GPO:** - Firewall aktiviert (alle Profile: Domain, Private, Public) - Inbound: Default Deny - Outbound: Default Allow (mit Ausnahmen)

**Erlaubte Inbound-Verbindungen:** - Remote Desktop (nur von Management-VLAN) - File Sharing (nur im Corporate Network) - Monitoring-Agents

### **61.4.2 4.2 macOS Firewall**

**Konfiguration via MDM:** - Application Firewall aktiviert - Stealth Mode aktiviert - Nur signierte Apps erlaubt

### **61.4.3 4.3 Linux Firewall**

**iptables/firewalld:** - Default Deny für Inbound - Nur erforderliche Services erlaubt - Logging aktiviert

## **61.5 5. Device Compliance**

### **61.5.1 5.1 Compliance-Anforderungen**

**Pflicht-Anforderungen:** - EDR/AV installiert und aktiv - OS-Patches aktuell (< 30 Tage alt) - Disk-Verschlüsselung aktiviert - Host-Firewall aktiviert - Screen-Lock konfiguriert (max. 15 Minuten) - Kein Jailbreak/Root (Mobile)

### **61.5.2 5.2 Compliance-Checks**

**Automatische Prüfung:** - Bei jedem Netzwerk-Zugriff (NAC) - Bei VPN-Verbindung - Täglich (Endpoint-Management)

**Bei Non-Compliance:** - Warnung an Nutzer (24 Stunden Frist) - Eingeschränkter Netzwerk-Zugriff - Vollständige Sperrung nach 7 Tagen

### **61.5.3 5.3 Compliance-Reporting**

**Wöchentlicher Report:** - Compliance-Rate pro Abteilung - Top Non-Compliance-Items - Trend-Analyse

**Ziel:** > 95% Compliance

## 61.6 6. Patch Management

### 61.6.1 6.1 OS-Patches

**Windows:** - WSUS für Patch-Verteilung - Automatische Installation (außerhalb Geschäftszeiten)  
- Reboot-Fenster: Wochenende

**macOS:** - Automatische Updates über MDM - Deferred Updates (7 Tage Test-Period)

**Linux:** - Automatische Security-Updates (unattended-upgrades) - Manuelle Updates für Kernel

### 61.6.2 6.2 Application-Patches

**Third-Party-Applications:** - Ninite, Chocolatey für automatische Updates - Manuelle Updates für kritische Apps

**Patch-SLA:** - Critical: 7 Tage - High: 30 Tage - Medium: 90 Tage

**Details:** Siehe 0350\_Richtlinie\_Vulnerability\_Scans\_Patching

## 61.7 7. Application Control

### 61.7.1 7.1 Application Whitelisting

**Für kritische Systeme:** - Nur signierte, genehmigte Anwendungen - Blockierung nicht genehmigter Software - Ausnahmen über Ticketsystem

**Tools:** - Windows Defender Application Control (WDAC) - AppLocker

### 61.7.2 7.2 Script Control

**PowerShell:** - Constrained Language Mode - Script-Signing erforderlich - Logging aktiviert

**CMD/Batch:** - Blockiert für Standard-Nutzer - Nur für Admins

## 61.8 8. USB und Removable Media

### 61.8.1 8.1 USB-Control

**Policies:** - USB-Storage blockiert (Standard-Nutzer) - Nur genehmigte USB-Geräte (Whitelist) - Automatisches Scannen bei Anschluss

**Ausnahmen:** - Antrag über Ticketsystem - Zeitlich befristet - Verschlüsselte USB-Sticks

### 61.8.2 8.2 DLP für Removable Media

**Data Loss Prevention:** - Blockierung vertraulicher Daten auf USB - Alerts bei Kopierversuchen  
- Logging aller USB-Aktivitäten

## 61.9 9. Monitoring und Alerting

### 61.9.1 9.1 Endpoint-Monitoring

**Überwachte Metriken:** - EDR/AV-Status - Patch-Level - Compliance-Status - Malware-Detektionen - Anomalien (CPU, Netzwerk)

### 61.9.2 9.2 SIEM-Integration

**Events zu SIEM:** - Malware-Detektionen - EDR-Alerts - Compliance-Violations - Tamper-Attempts

### 61.9.3 9.3 Automated Response

**SOAR-Integration:** - Automatische Isolation bei Malware - Automatische Ticket-Erstellung - Automatische Benachrichtigungen

## 61.10 10. Compliance und Audit

### 61.10.1 10.1 Messgrößen (KPIs)

Metrik	Zielwert
EDR-Deployment-Rate	100%
AV-Signature-Aktualität	100%
Device-Compliance-Rate	> 95%
Malware-Detection-Rate	Baseline
Patch-Compliance (30 Tage)	> 90%

### 61.10.2 10.2 Audit-Nachweise

- EDR-Deployment-Status
- Compliance-Reports
- Malware-Incident-Reports
- Patch-Compliance-Reports

## 61.11 11. Referenzen

### 61.11.1 Interne Dokumente

- 0620\_Policy\_Endpoint\_Security.md
- 0350\_Richtlinie\_Vulnerability\_Scans\_Patching\_und\_Exploitation\_Response.md

### 61.11.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.8.7 - Protection against malware
- NIST SP 800-83 - Guide to Malware Incident Prevention and Handling
- CIS Controls - Malware Defenses

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 62

## Policy: Ausnahmen und Risk Waivers

**Dokument-ID:** 0640

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.1, A.6.1.2 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 62.1 1. Zweck

Diese Policy definiert den Prozess für Ausnahmen (Exceptions) und Risk Waivers von Sicherheitsrichtlinien der **AdminSend GmbH**. Sie stellt sicher, dass Ausnahmen angemessen begründet, genehmigt, dokumentiert und überwacht werden.

### 62.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Policies:** Alle Sicherheitsrichtlinien und -standards
- **Systeme:** Alle IT-Systeme und Anwendungen
- **Prozesse:** Alle sicherheitsrelevanten Prozesse
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Diese Policy selbst unterliegt keinem Ausnahmenprozess.

## 62.3 3. Grundsätze (Policy Statements)

### 62.3.1 3.1 Ausnahmen als Ausnahme

Ausnahmen von Sicherheitsrichtlinien sind die Ausnahme, nicht die Regel. Richtlinien sind grundsätzlich einzuhalten.

### 62.3.2 3.2 Formaler Ausnahmenprozess

Ausnahmen müssen über einen formalen Prozess beantragt werden. Informelle oder mündliche Ausnahmen sind nicht zulässig.

### 62.3.3 3.3 Begründungspflicht

Jede Ausnahme muss begründet werden: - Geschäftliche Notwendigkeit - Technische Unmöglichkeit - Unverhältnismäßiger Aufwand - Zeitliche Befristung

### 62.3.4 3.4 Risikobewertung

Für jede Ausnahme wird eine Risikobewertung durchgeführt. Risiken werden identifiziert, bewertet und dokumentiert.

### 62.3.5 3.5 Kompensationsmaßnahmen

Ausnahmen erfordern Kompensationsmaßnahmen. Kompensationsmaßnahmen reduzieren das Restrisiko auf ein akzeptables Niveau.

### 62.3.6 3.6 Genehmigungspflicht

Ausnahmen müssen von autorisierten Personen genehmigt werden: - **Low Risk:** CISO oder Stellvertreter - **Medium Risk:** CISO + Business Owner - **High Risk:** CISO + CIO + Management

### 62.3.7 3.7 Zeitliche Befristung

Ausnahmen sind grundsätzlich zeitlich befristet. Maximale Laufzeit: 12 Monate. Verlängerungen erfordern erneute Genehmigung.

### 62.3.8 3.8 Dokumentation

Alle Ausnahmen werden zentral dokumentiert (Ausnahmenregister). Dokumentation umfasst: - Antragsteller und Datum - Betroffene Policy/Standard - Begründung - Risikobewertung - Kompensationsmaßnahmen - Genehmiger und Datum - Laufzeit und Review-Datum

### 62.3.9 3.9 Monitoring und Review

Ausnahmen werden regelmäßig überprüft (mindestens quartalsweise). Nicht mehr benötigte Ausnahmen werden zurückgezogen.

## 62.4 4. Rollen und Verantwortlichkeiten

### 62.4.1 RACI-Matrix: Ausnahmen und Risk Waivers

Aktivität	CISO	CIO	Business Owner	Risk Manager	ISMS Team
Policy-Erstellung	R/A	C	C	C	C
Ausnahmenantrag	I	I	R	I	C
Risikobewertung	R/A	C	C	R	C
Kompensationsmaßnahmen	R/A	C	R	C	C
Genehmigung (Low)	R/A	I	I	I	I
Genehmigung (Medium)	R/A	I	R/A	C	I
Genehmigung (High)	R/A	R/A	R/A	C	I
Ausnahmenregister	C	I	I	C	R/A
Monitoring & Review	R/A	C	C	C	R

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

### 62.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **CIO:** Anna Schmidt
- **Risk Manager:** {{ meta.risk.manager }}
- **ISMS Team:** {{ meta.isms.team }}
- **Antragsteller:** Business Owner, IT-Betrieb
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit

## 62.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

### 62.5.1 Zugehörige Richtlinien

- **0650\_Richtlinie\_Ausnahmenprozess.md** - Detaillierte Implementierungsrichtlinie
- **0060\_ISMS\_Risikomanagement\_Methodik.md** - Risk Management Methodology
- **0080\_ISMS\_Risikoregister\_Template.md** - Risk Register

### 62.5.2 Zugehörige Standards/Baselinses

- Ausnahmenantrag-Template
- Risikobewertungs-Template
- Kompensationsmaßnahmen-Katalog
- Ausnahmenregister

### 62.5.3 Zugehörige Prozesse

- Ausnahmenantragsprozess
- Risikobewertungsprozess

- Genehmigungsprozess
- Monitoring und Review Prozess

## 62.6 6. Compliance, Monitoring und Durchsetzung

### 62.6.1 Messgrößen und KPIs

- Anzahl aktiver Ausnahmen
- Durchschnittliche Laufzeit von Ausnahmen
- Anzahl abgelaufener Ausnahmen (Ziel: 0)
- Anzahl verlängerter Ausnahmen
- Ausnahmen nach Risikokategorie (Low/Medium/High)
- Review-Compliance (Ziel: 100% quartalsweise)
- Anzahl zurückgezogener Ausnahmen

### 62.6.2 Nachweise und Evidence

- Ausnahmenregister
- Ausnahmenanträge und Genehmigungen
- Risikobewertungen
- Kompensationsmaßnahmen-Dokumentation
- Review-Protokolle
- Audit Logs für Ausnahmen

### 62.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:

- **Nicht genehmigte Ausnahmen:** Sofortige Compliance-Herstellung oder Systemabschaltung
- **Fehlende Dokumentation:** Nachholung, Compliance-Untersuchung
- **Abgelaufene Ausnahmen:** Sofortige Compliance-Herstellung oder Verlängerungsantrag
- **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen, Eskalation an Management

## 62.7 7. Ausnahmen

Diese Policy selbst unterliegt keinem Ausnahmenprozess. Änderungen an dieser Policy erfordern Management-Genehmigung.

## 62.8 8. Referenzen

### 62.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0650\_Richtlinie\_Ausnahmenprozess.md - Detailed Guideline
- 0060\_ISMS\_Risikomanagement\_Methodik.md - Risk Management Methodology
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

### 62.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.5.1 - Policies for information security

- ISO/IEC 27001:2022 Annex A.6.1.2 - Segregation of duties
  - ISO/IEC 27005 - Information security risk management
  - NIST SP 800-37 - Risk Management Framework
  - COBIT 2019 - APO12 (Managed Risk)
- 

**Genehmigt durch:**

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 63

## Richtlinie: Ausnahmenprozess

**Dokument-ID:** 0650

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.1

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 63.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md und definiert: - Ausnahmenprozess für Security-Policies - Risk-Waiver-Verfahren - Kompensationskontrollen

**Geltungsbereich:** Alle Security-Policies bei AdminSend GmbH

### 63.2 2. Ausnahmen-Kategorien

#### 63.2.1 2.1 Temporäre Ausnahmen

**Definition:** Zeitlich befristete Abweichung von Policy

**Beispiele:** - Verzögertes Patching (wegen Kompatibilitätsproblemen) - Temporäre Firewall-Regel für Projekt - Verzögerte Compliance (während Migration)

**Maximale Dauer:** 12 Monate

#### 63.2.2 2.2 Permanente Ausnahmen

**Definition:** Dauerhafte Abweichung von Policy

**Beispiele:** - Legacy-Systeme, die Baseline nicht erfüllen können - Spezielle Geschäftsanforderungen - Technische Unmöglichkeit

**Review-Frequenz:** Jährlich

### 63.2.3 2.3 Notfall-Ausnahmen

**Definition:** Sofortige Ausnahme bei Notfällen

**Beispiele:** - Kritische Business-Anforderung - Systemausfall-Behebung - Security-Incident-Response

**Nachträgliche Genehmigung:** Innerhalb 48 Stunden

## 63.3 3. Ausnahmenprozess

### 63.3.1 3.1 Antragstellung

**Antrag über:** {{ meta.itsm.portal }} (Ticketsystem)

**Pflichtangaben:** - Betroffene Policy/Richtlinie - Beschreibung der Abweichung - Begründung (Business Justification) - Betroffene Systeme/Prozesse - Risikobewertung - Vorgeschlagene Kompensationskontrollen - Gewünschte Dauer

**Antragsteller:** System-Owner oder Fachbereichsleiter

### 63.3.2 3.2 Risikobewertung

**Durchführung durch:** IT-Security-Team

**Bewertungskriterien:** - Wahrscheinlichkeit eines Sicherheitsvorfalls - Potenzielle Auswirkungen - Betroffene Assets und Daten - Bestehende Kontrollen - Vorgeschlagene Kompensationskontrollen

**Risiko-Matrix:** | Wahrscheinlichkeit | Auswirkung Niedrig | Auswirkung Mittel | Auswirkung Hoch | |-----|-----|-----|-----| | Niedrig | Niedrig | Niedrig | Mittel | | Mittel | Niedrig | Mittel | Hoch | | Hoch | Mittel | Hoch | Kritisch |

### 63.3.3 3.3 Kompensationskontrollen

**Definition:** Alternative Sicherheitsmaßnahmen zur Risikominimierung

**Beispiele:** - Netzwerk-Isolation (bei fehlenden Patches) - Erhöhtes Monitoring (bei schwächerer Authentifizierung) - Manuelle Prozesse (bei fehlender Automatisierung) - Zusätzliche Zugriffsbeschränkungen

**Anforderung:** - Kompensationskontrollen müssen Risiko auf akzeptables Niveau senken - Dokumentation der Wirksamkeit

### 63.3.4 3.4 Genehmigung

**Genehmigungsstufen:**

Risiko	Genehmiger	SLA
Niedrig	IT-Security-Manager	3 Arbeitstage
Mittel	CISO	5 Arbeitstage
Hoch	CISO + CIO	7 Arbeitstage

Risiko	Genehmiger	SLA
Kritisch	CISO + CIO + Geschäftsführung	10 Arbeitstage

**Genehmigungskriterien:** - Business Justification nachvollziehbar - Risiko akzeptabel (mit Kompensationskontrollen) - Keine Alternative verfügbar - Zeitlich befristet (bei temporären Ausnahmen)

**Ablehnung:** - Begründung erforderlich - Alternative Lösungen vorschlagen

### 63.3.5 3.5 Dokumentation

**Ausnahmen-Register:** - Alle genehmigten Ausnahmen - Antragsteller, Genehmiger, Datum - Risikobewertung - Kompensationskontrollen - Ablaufdatum - Review-Datum

**Speicherort:** {{ meta.compliance.exception\_register }}

## 63.4 4. Monitoring und Review

### 63.4.1 4.1 Laufende Überwachung

**Verantwortlichkeit:** IT-Security-Team

**Aktivitäten:** - Wirksamkeit der Kompensationskontrollen prüfen - Compliance mit Ausnahmen-Bedingungen - Incidents im Zusammenhang mit Ausnahmen

**Frequenz:** Monatlich (bei kritischen Ausnahmen), quartalsweise (bei anderen)

### 63.4.2 4.2 Regelmäßiger Review

**Temporäre Ausnahmen:** - Review 30 Tage vor Ablauf - Entscheidung: Verlängern, Beenden, Permanent machen

**Permanente Ausnahmen:** - Jährlicher Review - Prüfung auf Notwendigkeit - Aktualisierung der Risikobewertung

**Notfall-Ausnahmen:** - Review innerhalb 7 Tage nach Genehmigung - Regularisierung oder Beendigung

### 63.4.3 4.3 Eskalation

**Bei Problemen:** - Kompensationskontrollen unwirksam - Risiko gestiegen - Incidents im Zusammenhang mit Ausnahme

**Eskalation an:** - CISO (sofort) - Risk Committee (bei kritischen Ausnahmen)

## 63.5 5. Beendigung von Ausnahmen

### 63.5.1 5.1 Geplante Beendigung

**Bei Ablauf:** 1. Benachrichtigung an Antragsteller (30 Tage vorher) 2. Remediation-Plan erstellen 3. Umsetzung der Remediation 4. Verifizierung 5. Ausnahme schließen

### **63.5.2 5.2 Vorzeitige Beendigung**

**Gründe:** - Risiko nicht mehr akzeptabel - Kompensationskontrollen unwirksam - Alternative Lösung verfügbar - Geschäftsanforderung entfallen

**Prozess:** 1. Entscheidung durch CISO 2. Benachrichtigung an Antragsteller 3. Sofortige Remediation (oder Systemabschaltung) 4. Dokumentation

## **63.6 6. Reporting**

### **63.6.1 6.1 Monatlicher Ausnahmen-Report**

**Inhalte:** - Anzahl aktiver Ausnahmen (nach Risiko) - Neue Ausnahmen im Monat - Abgelaufene Ausnahmen - Überfällige Reviews - Top-Ausnahmen nach Risiko

**Empfänger:** CISO, CIO, Risk Committee

### **63.6.2 6.2 Quartalsweiser Management-Report**

**Inhalte:** - Trend-Analyse - Ausnahmen nach Kategorie/Abteilung - Risiko-Posture - Verbesserungsmaßnahmen

**Empfänger:** Geschäftsführung, Audit Committee

## **63.7 7. Compliance und Audit**

### **63.7.1 7.1 Messgrößen (KPIs)**

Metrik	Zielwert
Ausnahmen mit aktuellem Review	100%
Überfällige Ausnahmen	0
Ausnahmen mit Kompensationskontrollen	100%
Durchschnittliche Ausnahmen-Dauer	< 6 Monate

### **63.7.2 7.2 Audit-Nachweise**

- Ausnahmen-Register
- Anträge und Genehmigungen
- Risikobewertungen
- Review-Protokolle
- Monitoring-Berichte

## **63.8 8. Beispiele**

### **63.8.1 8.1 Beispiel: Verzögertes Patching**

**Szenario:** Kritischer Patch verursacht Kompatibilitätsprobleme mit Business-Anwendung

**Antrag:** - Policy: Patch Management (Critical Patches innerhalb 7 Tage) - Abweichung: Verzögerung um 30 Tage - Begründung: Kompatibilitätsproblem, Vendor arbeitet an Fix - Risiko: Hoch (bekannter Exploit)

**Kompensationskontrollen:** - Netzwerk-Isolation des betroffenen Systems - IPS-Signatur aktiviert  
- Erhöhtes Monitoring - Zugriffsbeschränkungen

**Genehmigung:** CISO + CIO

**Dauer:** 30 Tage

**Review:** Wöchentlich

### 63.8.2 8.2 Beispiel: Legacy-System

**Szenario:** Legacy-System kann Security-Baseline nicht erfüllen

**Antrag:** - Policy: Security-Baseline (CIS Benchmark Level 1) - Abweichung: Veraltetes OS, keine Patches mehr verfügbar - Begründung: Kritische Business-Anwendung, keine Migration möglich (kurzfristig) - Risiko: Hoch

**Kompensationskontrollen:** - Dediziertes VLAN (isoliert) - Firewall-Regeln (nur erforderliche Verbindungen) - Kein Internet-Zugriff - Read-Only-Zugriff für Standard-Nutzer - Erhöhtes Monitoring und Logging - Jährliche Penetration-Tests

**Genehmigung:** CISO + CIO + Geschäftsführung

**Dauer:** Permanent (bis Migration)

**Review:** Jährlich

## 63.9 9. Referenzen

### 63.9.1 Interne Dokumente

- 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- Alle Security-Policies und -Richtlinien

### 63.9.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.5.1 - Policies for information security
- NIST SP 800-53 - Security and Privacy Controls (Tailoring)

---

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 64

## Policy: Informationsübertragung und Kommunikation

**Dokument-ID:** 0660

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.14, A.8.24, A.8.26 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 64.1 1. Zweck

Diese Policy definiert die Anforderungen an die sichere Informationsübertragung und Kommunikation der **AdminSend GmbH**. Sie stellt sicher, dass Informationen während der Übertragung angemessen geschützt werden und Kommunikationskanäle sicher sind.

### 64.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Kommunikationskanäle:** E-Mail, Messaging, File Sharing, Collaboration Tools
- **Daten:** Alle Informationen (insbesondere vertrauliche und personenbezogene Daten)
- **Übertragungswege:** Intern, extern, Cloud, Partner
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_) zulässig.

## **64.3 3. Grundsätze (Policy Statements)**

### **64.3.1 3.1 Verschlüsselte Übertragung**

Vertrauliche Informationen werden verschlüsselt übertragen. Verschlüsselung erfolgt in Transit (TLS/SSL) und at Rest.

### **64.3.2 3.2 E-Mail-Sicherheit**

E-Mail-Kommunikation ist gesichert: - **Inbound:** SPF, DKIM, DMARC, Anti-Spam, Anti-Malware - **Outbound:** TLS-Verschlüsselung, S/MIME oder PGP für vertrauliche Inhalte - **Phishing-Schutz:** User Awareness, technische Schutzmaßnahmen

### **64.3.3 3.3 Sichere File Sharing**

File Sharing erfolgt über genehmigte Plattformen. Vertrauliche Dateien werden verschlüsselt geteilt. Public File Sharing (z.B. WeTransfer) ist für vertrauliche Daten untersagt.

### **64.3.4 3.4 Collaboration Tools**

Collaboration Tools (Teams, Slack, etc.) müssen Sicherheitsanforderungen erfüllen: - Verschlüsselte Kommunikation - Zugriffskontrolle - Data Loss Prevention (DLP) - Audit Logging

### **64.3.5 3.5 Messaging und Chat**

Instant Messaging für geschäftliche Kommunikation erfolgt über genehmigte Tools. Private Messaging-Apps sind für vertrauliche Geschäftsinformationen untersagt.

### **64.3.6 3.6 Data Loss Prevention (DLP)**

DLP-Systeme verhindern unbeabsichtigte oder böswillige Datenexfiltration. DLP überwacht E-Mail, File Sharing und Collaboration Tools.

### **64.3.7 3.7 Externe Kommunikation**

Kommunikation mit externen Parteien (Kunden, Partner, Lieferanten) erfolgt über sichere Kanäle. Vertraulichkeitsvereinbarungen (NDAs) werden bei Bedarf abgeschlossen.

### **64.3.8 3.8 Mobile Kommunikation**

Mobile Kommunikation (Smartphones, Tablets) erfolgt über sichere Kanäle. Mobile Geräte sind mit MDM/MAM verwaltet (siehe 0500\_Policy\_Mobile\_Device\_und\_Remote\_Work.md).

### **64.3.9 3.9 Social Media**

Geschäftliche Social-Media-Nutzung folgt Social-Media-Richtlinien. Vertrauliche Informationen werden nicht über Social Media geteilt.

## 64.4 4. Rollen und Verantwortlichkeiten

### 64.4.1 RACI-Matrix: Informationsübertragung und Kommunikation

Aktivität	CISO	IT-Betrieb	Communication Security	End User	DPO
Policy-Erstellung	R/A	C	R	I	C
E-Mail-Security	C	R/A	R	I	C
File Sharing	C	R/A	R	R	C
Collaboration Tools	C	R/A	R	R	C
DLP-Implementierung	R/A	R	R	I	C
Externe Kommunikation	C	C	C	R	C
Mobile Kommunikation	C	R/A	C	R	I
Social Media	C	I	R/A	R	I

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

### 64.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **Communication Security Manager:** {{ meta.communication.security\_manager }}
- **IT Operations Manager:** {{ meta.it.operations\_manager }}
- **Data Protection Officer:** {{ meta.dpo.name }}
- **Umsetzungsverantwortliche:** IT-Betrieb, End Users
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit, DPO

## 64.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

### 64.5.1 Zugehörige Richtlinien

- **0670\_Richtlinie\_Email\_Sharing\_und\_Zusammenarbeitstools.md** - Detaillierte Implementierungsrichtlinie
- **0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md** - Data Classification Policy
- **0260\_Policy\_Kryptografie\_und\_Schluesselmanagement.md** - Encryption Policy
- **0500\_Policy\_Mobile\_Device\_und\_Remote\_Work.md** - Mobile Device Policy

### 64.5.2 Zugehörige Standards/Baselines

- E-Mail-Security-Konfiguration (SPF, DKIM, DMARC)

- Genehmigte File-Sharing-Plattformen
- Genehmigte Collaboration Tools
- DLP-Regeln und -Policies
- Social-Media-Richtlinien

#### 64.5.3 Zugehörige Prozesse

- E-Mail-Verschlüsselungsprozess (S/MIME, PGP)
- File-Sharing-Genehmigungsprozess
- DLP-Incident-Response
- Externe Kommunikation (NDA-Prozess)

### 64.6 6. Compliance, Monitoring und Durchsetzung

#### 64.6.1 Messgrößen und KPIs

- E-Mail-Verschlüsselungsrate (Ziel: 100% für vertrauliche E-Mails)
- SPF/DKIM/DMARC-Compliance (Ziel: 100%)
- DLP-Incident-Rate
- Anzahl blockierter Phishing-E-Mails
- File-Sharing-Compliance (Ziel: 100% genehmigte Plattformen)
- Collaboration-Tool-Compliance
- Anzahl Social-Media-Verstöße

#### 64.6.2 Nachweise und Evidence

- E-Mail-Security-Konfiguration (SPF, DKIM, DMARC)
- E-Mail-Verschlüsselungsprotokolle
- DLP-Logs und Incident-Reports
- File-Sharing-Logs
- Collaboration-Tool-Konfiguration
- Phishing-Simulation-Ergebnisse
- Social-Media-Monitoring

#### 64.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:

- **Unverschlüsselte vertrauliche E-Mails:** Incident Response, User Awareness Training - **Nicht genehmigte File-Sharing-Tools:** Zugriff blockiert, Disziplinarmaßnahmen - **DLP-Verstöße:** Incident Response, Untersuchung, ggf. Disziplinarmaßnahmen - **Wiederholte Verstöße:** Arbeitssrechtliche Konsequenzen, Zugriffsentzug

### 64.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und Communication Security Manager genehmigt werden

- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet

## 64.8 8. Referenzen

### 64.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0670\_Richtlinie\_Email\_Sharing\_und\_Zusammenarbeitstools.md - Detailed Guideline
- 0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md - Data Classification Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

### 64.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.5.14 - Information transfer
  - ISO/IEC 27001:2022 Annex A.8.24 - Use of cryptography
  - ISO/IEC 27001:2022 Annex A.8.26 - Application security requirements
  - NIST SP 800-177 - Trustworthy Email
  - RFC 7208 - Sender Policy Framework (SPF)
  - RFC 6376 - DomainKeys Identified Mail (DKIM)
  - RFC 7489 - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- 

**Genehmigt durch:**

{{ meta.management.ceo }}, Geschäftsführung  
Datum: {{ meta.document.approval\_date }}

**Nächster Review:** {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 65

## Richtlinie: E-Mail, Sharing und Zusammenarbeitstools

**Dokument-ID:** 0670

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0660\_Policy\_Informationsuebertragung\_und\_Kommunikation.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.14

**Owner:** {{ meta.it\_operations.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 65.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0660\_Policy\_Informationsuebertragung\_und\_Kommunikation.md und definiert: - E-Mail-Sicherheit und -Nutzung - File-Sharing und Collaboration-Tools - Sichere Kommunikationskanäle

**Geltungsbereich:** Alle Kommunikationstools bei **AdminSend GmbH**

### 65.2 2. E-Mail-Sicherheit

#### 65.2.1 2.1 E-Mail-System

**Plattform:** {{ meta.email.system }} (z.B. Microsoft 365, Google Workspace)

**Sicherheitsfeatures:** - SPF, DKIM, DMARC konfiguriert - TLS für Transport-Verschlüsselung - Anti-Spam und Anti-Malware - DLP (Data Loss Prevention) - E-Mail-Archivierung

#### 65.2.2 2.2 E-Mail-Nutzung

**Erlaubte Nutzung:** - Geschäftliche Kommunikation - Begrenzte private Nutzung (max. 10 E-Mails/Tag) - Anmeldung bei geschäftlichen Online-Diensten

**Verbotene Aktivitäten:** - Versand vertraulicher Daten ohne Verschlüsselung - Spam, Ketten-mails - Nutzung privater E-Mail für geschäftliche Zwecke - Automatische Weiterleitung an externe Adressen

**Details:** Siehe 0210\_Richtlinie\_Akzeptable\_Nutzung\_IT.md

### 65.2.3 2.3 E-Mail-Verschlüsselung

**S/MIME:** - Für vertrauliche E-Mails verpflichtend - Zertifikate für alle Mitarbeiter - Automatische Verschlüsselung bei "Vertraulich"-Label

**Opportunistic TLS:** - Für alle ausgehenden E-Mails - MTA-STS für bekannte Partner

**Details:** Siehe 0270\_Richtlinie\_Key\_Management\_und\_Verschluesselung.md

### 65.2.4 2.4 Phishing-Schutz

**Technische Kontrollen:** - E-Mail-Gateway mit Anti-Phishing - Link-Rewriting und Sandbox - Attachment-Scanning - DMARC-Enforcement

**Nutzer-Schulung:** - Phishing-Awareness-Training (jährlich) - Phishing-Simulationen (quartalsweise) - Reporting-Button in E-Mail-Client

**Bei Phishing-Verdacht:** 1. E-Mail nicht öffnen/anklicken 2. Melden über Reporting-Button 3. E-Mail löschen 4. IT-Security prüft und reagiert

### 65.2.5 2.5 E-Mail-Archivierung

**Automatische Archivierung:** - Alle geschäftlichen E-Mails - Retention: {{ meta.retention.email\_years }} Jahre - Unveränderbarkeit (WORM)

**Zugriff:** - Nutzer: Eigene E-Mails - Legal/Compliance: Für eDiscovery - Vorgesetzte: Mit Genehmigung

**Details:** Siehe 0590\_Richtlinie\_Records\_Retention

## 65.3 3. File-Sharing

### 65.3.1 3.1 Genehmigte Plattformen

**Intern:** - **File-Server:** {{ netbox.device.fileservice }} - **SharePoint/OneDrive:** {{ meta.collaboration.sharepoint }} - **Teams/Slack:** {{ meta.collaboration.teams }}

**Extern (mit Kunden/Partnern):** - **Secure File Transfer:** {{ meta.filesharing.secure\_platform }} - **Nur mit Verschlüsselung und Passwortschutz**

**Verboten:** - Private Cloud-Dienste (Dropbox privat, Google Drive privat) - WeTransfer, Filemail (ohne Genehmigung) - USB-Sticks für vertrauliche Daten

### 65.3.2 3.2 Berechtigungen

**Least Privilege:** - Nur erforderliche Berechtigungen - Read-Only wo möglich - Zeitlich befristete Freigaben

**Externe Freigaben:** - Genehmigung durch Daten-Owner - Passwortschutz verpflichtend - Ablaufdatum setzen (max. 90 Tage) - Logging aller Zugriffe

### 65.3.3 3.3 DLP für File-Sharing

**Automatische Kontrollen:** - Blockierung vertraulicher Daten bei externer Freigabe - Warnung bei großen Datenmengen - Alerts bei ungewöhnlichen Sharing-Mustern

## 65.4 4. Collaboration-Tools

### 65.4.1 4.1 Microsoft Teams / Slack

**Genehmigte Nutzung:** - Interne Kommunikation - Projekt-Collaboration - Video-Konferenzen

**Sicherheitseinstellungen:** - Externe Gäste nur mit Genehmigung - DLP-Policies aktiviert - Retention-Policies konfiguriert - Audit-Logging aktiviert

**Verbotene Aktivitäten:** - Sharing vertraulicher Daten in öffentlichen Channels - Nutzung privater Accounts für geschäftliche Zwecke - Installation nicht genehmigter Apps/Bots

### 65.4.2 4.2 Video-Konferenzen

**Genehmigte Plattformen:** - **Intern:** {{ meta.collaboration.video }} (z.B. Teams, Zoom) - **Extern:** Nur genehmigte Plattformen

**Sicherheitseinstellungen:** - Warteraum aktiviert - Passwortschutz für Meetings - Keine Aufzeichnung ohne Zustimmung - Bildschirmfreigabe nur für Moderator

**Best Practices:** - Hintergrund-Unschärfe nutzen - Mikrofon stumm schalten wenn nicht sprechend - Keine vertraulichen Informationen in öffentlichen Meetings

### 65.4.3 4.3 Instant Messaging

**Genehmigte Tools:** - Microsoft Teams Chat - Slack (Enterprise)

**Verboten:** - WhatsApp, Telegram für geschäftliche Kommunikation - Private Messaging-Apps

**Retention:** - Chat-Historie: {{ meta.retention.chat\_years }} Jahre - Compliance-Archivierung

## 65.5 5. Externe Kommunikation

### 65.5.1 5.1 Kommunikation mit Kunden

**Kanäle:** - E-Mail (bevorzugt) - Telefon - Video-Konferenz - Kundenportal (falls vorhanden)

**Vertrauliche Informationen:** - Verschlüsselung verpflichtend - Secure File Transfer nutzen - Keine vertraulichen Daten per SMS/WhatsApp

### 65.5.2 5.2 Kommunikation mit Lieferanten

**Anforderungen:** - NDA vor Austausch vertraulicher Informationen - Genehmigte Kommunikationskanäle - Dokumentation wichtiger Kommunikation

### 65.5.3 5.3 Social Media

**Geschäftliche Nutzung:** - Nur autorisierte Accounts - Social Media Guidelines befolgen - Keine vertraulichen Informationen

**Private Nutzung:** - Keine Vortäuschung offizieller Unternehmensmeinung - Disclaimer bei Meinungsäußerungen - Keine negativen Äußerungen über Unternehmen

**Details:** Siehe 0210\_Richtlinie\_Akzeptable\_Nutzung\_IT.md

## 65.6 6. Mobile Kommunikation

### 65.6.1 6.1 Geschäfts-Smartphones

**Konfiguration:** - MDM-Enrollment verpflichtend - Verschlüsselung aktiviert - Remote-Wipe-Fähigkeit - Genehmigte Apps nur

**Nutzung:** - Geschäftliche E-Mails und Kalender - Teams/Slack - Geschäftliche Telefonate

### 65.6.2 6.2 BYOD

**Anforderungen:** - Containerisierung (Work Profile) - Separate Apps für geschäftlich/privat - MDM-Enrollment

**Details:** Siehe 0510\_Richtlinie\_MDM\_BringYourOwnDevice

## 65.7 7. Data Loss Prevention (DLP)

### 65.7.1 7.1 DLP-Policies

**Für E-Mail:** - Blockierung von Kreditkartenzahlen - Warnung bei "Vertraulich"-Label extern - Blockierung großer Anhänge (> 25 MB)

**Für File-Sharing:** - Blockierung vertraulicher Daten bei externer Freigabe - Warnung bei Sharing mit vielen Personen

**Für Collaboration-Tools:** - Warnung bei Posting vertraulicher Daten in öffentlichen Channels

### 65.7.2 7.2 DLP-Incidents

**Bei DLP-Blockierung:** 1. Nutzer erhält Warnung 2. Incident-Ticket erstellt 3. Security-Team prüft 4. Bei Bedarf: Schulung oder Disziplinarmaßnahmen

## 65.8 8. Compliance und Audit

### 65.8.1 8.1 Messgrößen (KPIs)

Metrik	Zielwert
E-Mail-Verschlüsselung (vertraulich)	100%
Phishing-Klickrate (Simulation)	< 5%
DLP-Incidents	< 10 pro Monat

Metrik	Zielwert
Externe Freigaben mit Passwort	100%

## 65.8.2 8.2 Audit-Nachweise

- E-Mail-Archiv
- File-Sharing-Logs
- DLP-Incident-Reports
- Phishing-Simulation-Ergebnisse

## 65.9 9. Referenzen

### 65.9.1 Interne Dokumente

- 0660\_Policy\_Informationsuebertragung\_und\_Kommunikation.md
- 0210\_Richtlinie\_Akzeptable\_Nutzung\_IT.md
- 0270\_Richtlinie\_Key\_Management\_und\_Verschluesselung.md

### 65.9.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.5.14 - Information transfer
- NIST SP 800-177 - Trustworthy Email

---

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 66

## Policy: Security in Projects

**Dokument-ID:** 0680

**Dokumenttyp:** Policy (abstrakt)

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.8, A.8.25, A.8.32 (inkl. Amendment 1:2024)

**Owner:** Thomas Weber

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

**Nächster Review:** {{ meta.document.next\_review }}

---

### 66.1 1. Zweck

Diese Policy definiert die Anforderungen an die Integration von Informationssicherheit in Projekte der **AdminSend GmbH**. Sie stellt sicher, dass Sicherheitsanforderungen im gesamten Projektlebenszyklus berücksichtigt werden.

### 66.2 2. Geltungsbereich

Diese Policy gilt für:

- **Organisationseinheiten:** Alle Abteilungen und Standorte der AdminSend GmbH
- **Projekte:** Alle IT-Projekte, Infrastrukturprojekte, Softwareentwicklungsprojekte
- **Projektphasen:** Initiierung, Planung, Umsetzung, Abschluss
- **Projektarten:** Interne Projekte, externe Projekte, Partnerprojekte
- **Standorte:** {{ netbox.site.name }} und alle weiteren Betriebsstandorte

**Ausnahmen:** Ausnahmen sind nur über den definierten Ausnahmenprozess (0640\_Policy\_Ausnahmen\_und\_Risk\_zulässig).

## **66.3 3. Grundsätze (Policy Statements)**

### **66.3.1 3.1 Security by Design**

Sicherheit wird von Anfang an in Projekte integriert (Security by Design). Sicherheitsanforderungen werden in der Projektinitiierung definiert.

### **66.3.2 3.2 Security Requirements**

Für jedes Projekt werden Sicherheitsanforderungen definiert: - Vertraulichkeit, Integrität, Verfügbarkeit - Compliance-Anforderungen - Datenschutzanforderungen - Technische Sicherheitsanforderungen

### **66.3.3 3.3 Security Risk Assessment**

Für jedes Projekt wird ein Security Risk Assessment durchgeführt. Risiken werden identifiziert, bewertet und behandelt.

### **66.3.4 3.4 Security Architecture Review**

Projektarchitekturen werden auf Sicherheit überprüft. Security Architecture Review erfolgt vor Implementierung.

### **66.3.5 3.5 Security Testing**

Projekte werden auf Sicherheit getestet: - Security Testing (Penetration Tests, Vulnerability Scans) - Code Reviews (SAST, DAST) für Softwareprojekte - Configuration Reviews für Infrastrukturprojekte

### **66.3.6 3.6 Security Sign-Off**

Projekte erhalten Security Sign-Off vor Go-Live. Security Sign-Off bestätigt, dass Sicherheitsanforderungen erfüllt sind.

### **66.3.7 3.7 Change Management Integration**

Sicherheitsrelevante Änderungen folgen dem Change-Management-Prozess (siehe 0360\_Policy\_Change\_und\_Relea

### **66.3.8 3.8 Third-Party Security**

Bei Projekten mit Drittparteien (Lieferanten, Partner) werden Sicherheitsanforderungen vertraglich vereinbart (siehe 0460\_Policy\_Lieferanten\_und\_Cloud\_Sicherheit.md).

### **66.3.9 3.9 Security Documentation**

Sicherheitsrelevante Projektdokumentation wird erstellt: - Security Requirements Specification - Security Architecture Document - Security Test Report - Security Sign-Off Document

## 66.4 4. Rollen und Verantwortlichkeiten

### 66.4.1 RACI-Matrix: Security in Projects

Aktivität	CISO	Project Manager	Security Architect	IT-Betrieb	Business Owner
Policy-Erstellung	R/A	C	R	C	C
Security Requirements	R	R/A	R	C	R
Security Risk Assessment	R/A	R	R	C	C
Security Architecture Review	R/A	C	R/A	C	C
Security Testing	R	R/A	R	R	C
Security Sign-Off	R/A	C	C	C	C
Change Management	C	R	C	R/A	C
Third-Party Security	R/A	R	C	C	R

**Legende:** R = Responsible (Durchführung), A = Accountable (Verantwortlich), C = Consulted (Konsultiert), I = Informed (Informiert)

### 66.4.2 Schlüsselrollen

- **Policy Owner:** Thomas Weber (CISO)
- **Security Architect:** {{ meta.security.architect }}
- **Project Manager:** Projektverantwortliche
- **IT Operations Manager:** {{ meta.it.operations\_manager }}
- **Business Owner:** Fachbereichsverantwortliche
- **Kontroll-/Prüfinstanz:** ISMS, Internal Audit

## 66.5 5. Ableitungen (Richtlinien/Standards/Prozesse)

Details zur Umsetzung werden in nachgelagerten Dokumenten geregelt:

### 66.5.1 Zugehörige Richtlinien

- **0690\_Richtlinie\_Sicherheitsanforderungen\_im\_Projektlebenszyklus.md** - Detaillierte Implementierungsrichtlinie

- 0380\_Policy\_Secure\_Development.md - Secure Development Policy
- 0360\_Policy\_Change\_und\_Release\_Management.md - Change Management Policy
- 0460\_Policy\_Lieferanten\_und\_Cloud\_Sicherheit.md - Supplier Security Policy

### 66.5.2 Zugehörige Standards/Baselinses

- Security Requirements Template
- Security Risk Assessment Template
- Security Architecture Review Checklist
- Security Testing Standards
- Security Sign-Off Template

### 66.5.3 Zugehörige Prozesse

- Project Security Review Prozess
- Security Risk Assessment Prozess
- Security Architecture Review Prozess
- Security Testing Prozess
- Security Sign-Off Prozess

## 66.6 6. Compliance, Monitoring und Durchsetzung

### 66.6.1 Messgrößen und KPIs

- Anzahl Projekte mit Security Requirements (Ziel: 100%)
- Anzahl durchgeföhrter Security Risk Assessments (Ziel: 100% aller Projekte)
- Anzahl Security Architecture Reviews (Ziel: 100% kritischer Projekte)
- Anzahl Security Tests (Ziel: 100% vor Go-Live)
- Anzahl Security Sign-Offs (Ziel: 100% vor Go-Live)
- Durchschnittliche Zeit für Security Review (Ziel: < 5 Tage)
- Anzahl Projekte ohne Security Sign-Off (Ziel: 0)

### 66.6.2 Nachweise und Evidence

- Security Requirements Specifications
- Security Risk Assessments
- Security Architecture Review Reports
- Security Test Reports (Penetration Tests, Vulnerability Scans)
- Security Sign-Off Documents
- Project Security Checklists
- Change Management Records

### 66.6.3 Konsequenzen bei Verstößen

Verstöße gegen diese Policy werden nach den geltenden HR- und Compliance-Prozessen behandelt:

- **Projekte ohne Security Requirements:** Projektstop bis Requirements definiert - **Fehlende Security Risk Assessments:** Nachholung vor Fortsetzung - **Go-Live ohne Security Sign-Off:** Projektstop, Eskalation an Management - **Wiederholte Verstöße:** Arbeitsrechtliche Konsequenzen, Projektverantwortung entzogen

## 66.7 7. Ausnahmen

Ausnahmen von dieser Policy sind nur in begründeten Ausnahmefällen zulässig:

- **Ausnahmenprozess:** Siehe 0640\_Policy\_Ausnahmen\_und\_Risk\_Waivers.md
- **Genehmigung:** Ausnahmen müssen vom CISO und CIO genehmigt werden
- **Dokumentation:** Alle Ausnahmen werden im Risikoregister dokumentiert
- **Befristung:** Ausnahmen sind grundsätzlich zeitlich befristet

## 66.8 8. Referenzen

### 66.8.1 Interne Dokumente

- 0010\_ISMS\_Informationssicherheitsleitlinie.md - ISMS Policy
- 0690\_Richtlinie\_Sicherheitsanforderungen\_im\_Projektlebenszyklus.md - Detailed Guideline
- 0380\_Policy\_Secure\_Development.md - Secure Development Policy
- 0080\_ISMS\_Risikoregister\_Template.md - Risk Register

### 66.8.2 Externe Standards und Vorgaben

- ISO/IEC 27001:2022 Annex A.5.8 - Information security in project management
- ISO/IEC 27001:2022 Annex A.8.25 - Secure development life cycle
- ISO/IEC 27001:2022 Annex A.8.32 - Change management
- NIST SP 800-64 - Security Considerations in the System Development Life Cycle
- OWASP SAMM - Software Assurance Maturity Model
- BSIMM - Building Security In Maturity Model
- ISO/IEC 27034 - Application Security

---

#### Genehmigt durch:

{{ meta.management.ceo }}, Geschäftsführung

Datum: {{ meta.document.approval\_date }}

Nächster Review: {{ meta.document.next\_review }} (jährlich oder anlassbezogen)

ewpage

# Chapter 67

## Richtlinie: Sicherheitsanforderungen im Projektlebenszyklus

**Dokument-ID:** 0690

**Dokumenttyp:** Richtlinie (detailliert)

**Zugehörige Policy:** 0680\_Policy\_Security\_in\_Projects.md

**Standard-Referenz:** ISO/IEC 27001:2022 Annex A.5.8

**Owner:** {{ meta.pmo.manager }}

**Version:** 1.0

**Status:** Freigegeben

**Klassifizierung:** Intern

**Letzte Aktualisierung:** {{ meta.document.date }}

---

### 67.1 1. Zweck und Geltungsbereich

Diese Richtlinie konkretisiert die 0680\_Policy\_Security\_in\_Projects.md und definiert:  
- Security-Anforderungen in allen Projektphasen  
- Security-Reviews und -Gateways  
- Security-by-Design-Prinzipien

**Geltungsbereich:** Alle IT-Projekte bei **AdminSend GmbH**

### 67.2 2. Projektklassifizierung

#### 67.2.1 2.1 Projekt-Kategorien

**Kategorie A (Kritisch):** - Neue Systeme mit vertraulichen Daten - Internet-facing Anwendungen  
- Kritische Infrastruktur - **Security-Involvement:** Umfassend

**Kategorie B (Hoch):** - Interne Anwendungen mit sensiblen Daten - Änderungen an kritischen Systemen - **Security-Involvement:** Detailliert

**Kategorie C (Standard):** - Standard-IT-Projekte - Infrastruktur-Upgrades - **Security-Involvement:** Standard

**Kategorie D (Niedrig):** - Kleine Änderungen - Nicht-kritische Systeme - **Security-Involvement:** Minimal

## 67.2.2 2.2 Klassifizierungskriterien

**Bewertung:** - Datenklassifizierung (Vertraulich/Streng Vertraulich = höhere Kategorie) - Internet-Exposition (Ja = höhere Kategorie) - Anzahl Nutzer (> 100 = höhere Kategorie) - Compliance-Anforderungen (DSGVO, PCI-DSS = höhere Kategorie)

# 67.3 3. Projektphasen und Security-Aktivitäten

## 67.3.1 3.1 Initiierung

**Security-Aktivitäten:** - Projekt-Klassifizierung - Security-Stakeholder identifizieren - Initiales Security-Budget

**Deliverables:** - Projekt-Klassifizierung - Security-Kontaktperson

**Security-Gateway:** Keine (Informativ)

## 67.3.2 3.2 Planung

**Security-Aktivitäten:** - Security-Anforderungen definieren - Threat Modeling (Kategorie A/B) - Datenschutz-Folgenabschätzung (DSFA) bei Bedarf - Security-Architektur-Review - Security-Testing-Plan

**Deliverables:** - Security-Requirements-Dokument - Threat Model (Kategorie A/B) - DSFA (falls erforderlich) - Security-Test-Plan

**Security-Gateway 1:** - **Kategorie A/B:** Verpflichtend - **Genehmiger:** CISO oder Security-Architekt - **Kriterien:** Security-Requirements vollständig, Threat Model akzeptabel

## 67.3.3 3.3 Design

**Security-Aktivitäten:** - Security-Architecture-Review - Secure-Design-Patterns anwenden - Authentifizierung/Autorisierung-Design - Verschlüsselungs-Design - Logging/Monitoring-Design

**Deliverables:** - Security-Architecture-Dokument - Data Flow Diagrams - Authentication/Authorization-Design

**Security-Gateway 2:** - **Kategorie A:** Verpflichtend - **Genehmiger:** CISO und Security-Architekt - **Kriterien:** Security-Architecture akzeptabel, keine kritischen Schwachstellen im Design

## 67.3.4 3.4 Entwicklung/Beschaffung

**Security-Aktivitäten (Entwicklung):** - Secure Coding Standards befolgen - Code-Reviews (inkl. Security-Review) - SAST (Static Application Security Testing) - Dependency-Scanning - Secrets-Management

**Security-Aktivitäten (Beschaffung):** - Vendor-Security-Assessment - Vertragsprüfung (Security-Klauseln) - Auftragsverarbeitungsvertrag (AVV) bei Bedarf

**Deliverables:** - Code-Review-Berichte - SAST-Berichte - Vendor-Assessment (bei Beschaffung)

**Details:** Siehe 0390\_Richtlinie\_Secure\_SDLC und 0470\_Richtlinie\_Third\_Party\_Risk\_Assessment

### 67.3.5 3.5 Testing

**Security-Testing:** - DAST (Dynamic Application Security Testing) - Penetration-Testing (Kategorie A/B) - Security-Test-Cases - Vulnerability-Scanning

**Deliverables:** - DAST-Berichte - Penetration-Test-Bericht (Kategorie A/B) - Security-Test-Ergebnisse

**Security-Gateway 3:** - Kategorie A/B: Verpflichtend - Genehmiger: CISO - Kriterien: Keine kritischen/hohen Schwachstellen, alle Security-Tests bestanden

### 67.3.6 3.6 Deployment

**Security-Aktivitäten:** - Security-Configuration-Review - Hardening gemäß Baseline - Firewall-Regeln konfigurieren - Monitoring/Alerting einrichten - Backup konfigurieren

**Deliverables:** - Security-Configuration-Checkliste - Firewall-Regeln-Dokumentation - Monitoring-Setup-Dokumentation

**Security-Gateway 4 (Go-Live):** - Kategorie A/B: Verpflichtend - Genehmiger: CISO - Kriterien: Security-Configuration korrekt, Monitoring aktiv, keine offenen kritischen Findings

### 67.3.7 3.7 Betrieb und Wartung

**Security-Aktivitäten:** - Regelmäßige Vulnerability-Scans - Patch-Management - Security-Incident-Monitoring - Jährlicher Security-Review (Kategorie A)

**Deliverables:** - Vulnerability-Scan-Berichte - Patch-Compliance-Berichte - Incident-Reports

### 67.3.8 3.8 Außerbetriebnahme

**Security-Aktivitäten:** - Daten-Backup (falls erforderlich) - Sichere Daten-Lösung - Zugriffe widerrufen - Firewall-Regeln entfernen - Dokumentation archivieren

**Deliverables:** - Löschprotokoll - Decommissioning-Checkliste

## 67.4 4. Security-by-Design-Prinzipien

### 67.4.1 4.1 Least Privilege

**Prinzip:** Minimale erforderliche Berechtigungen

**Umsetzung:** - Rollenbasierte Zugriffskontrolle (RBAC) - Keine Default-Admin-Accounts - Just-in-Time (JIT) Access für privilegierte Operationen

### 67.4.2 4.2 Defense in Depth

**Prinzip:** Mehrere Sicherheitsschichten

**Umsetzung:** - Netzwerk-Segmentierung - Firewall + IDS/IPS - Endpoint-Protection + EDR - Application-Security + WAF

#### 67.4.3 4.3 Fail Secure

**Prinzip:** Bei Fehler in sicheren Zustand

**Umsetzung:** - Default Deny (Firewall, Zugriffskontrolle) - Fehler führen zu Zugriffsverweigerung (nicht Zugriff) - Graceful Degradation

#### 67.4.4 4.4 Privacy by Design

**Prinzip:** Datenschutz von Anfang an

**Umsetzung:** - Datenminimierung - Zweckbindung - Verschlüsselung - Anonymisierung/Pseudonymisierung

**Details:** Siehe 0570\_Richtlinie\_Datenschutz\_Anforderungen

### 67.5 5. Security-Requirements

#### 67.5.1 5.1 Funktionale Security-Requirements

**Authentifizierung:** - Multi-Faktor-Authentifizierung (MFA) für externe Zugriffe - Starke Passwörter oder Zertifikate - Session-Management

**Autorisierung:** - Rollenbasierte Zugriffskontrolle (RBAC) - Least Privilege - Segregation of Duties

**Verschlüsselung:** - TLS 1.2+ für Datenübertragung - AES-256 für Daten in Ruhe - Sichere Schlüsselverwaltung

**Logging:** - Authentifizierungs-Events - Zugriffe auf vertrauliche Daten - Administrative Aktionen - Fehler und Exceptions

#### 67.5.2 5.2 Nicht-funktionale Security-Requirements

**Performance:** - Security-Kontrollen dürfen Performance nicht signifikant beeinträchtigen (< 10%)

**Verfügbarkeit:** - Security-Kontrollen hochverfügbar - Failover-Mechanismen

**Wartbarkeit:** - Security-Konfiguration dokumentiert - Automatisierte Security-Tests

### 67.6 6. Threat Modeling

#### 67.6.1 6.1 Methodik

**STRIDE:** - Spoofing (Identitätsfälschung) - Tampering (Manipulation) - Repudiation (Abstreitbarkeit) - Information Disclosure (Informationspreisgabe) - Denial of Service (Dienstverweigerung) - Elevation of Privilege (Rechteausweitung)

#### 67.6.2 6.2 Prozess

**Schritte:** 1. System-Architektur dokumentieren (Data Flow Diagrams) 2. Bedrohungen identifizieren (STRIDE) 3. Bedrohungen bewerten (Risiko) 4. Mitigationsmaßnahmen definieren 5. Dokumentation

**Tool:** {{ meta.security.threat\_modeling\_tool }} (z.B. Microsoft Threat Modeling Tool)

## 67.7 7. Security-Testing

### 67.7.1 7.1 Test-Typen

**SAST (Static Application Security Testing):** - Während Entwicklung - Automatisiert in CI/CD - Fokus: Code-Schwachstellen

**DAST (Dynamic Application Security Testing):** - Während Testing-Phase - Automatisiert oder manuell - Fokus: Laufzeit-Schwachstellen

**Penetration-Testing:** - Vor Go-Live (Kategorie A/B) - Manuell durch Experten - Fokus: Realistische Angriffs-Szenarien

**Details:** Siehe 0390\_Richtlinie\_Secure\_SDLC

### 67.7.2 7.2 Remediation

**Prozess:** 1. Findings priorisieren (nach CVSS) 2. Remediation-Plan erstellen 3. Fixes implementieren 4. Re-Test 5. Dokumentation

**SLA:** - Critical: Vor Go-Live - High: Vor Go-Live oder mit Kompensationskontrollen - Medium: Innerhalb 30 Tage nach Go-Live - Low: Innerhalb 90 Tage nach Go-Live

## 67.8 8. Compliance und Audit

### 67.8.1 8.1 Messgrößen (KPIs)

Metrik	Zielwert
Security-Gateway-Compliance (Kategorie A/B)	100%
Penetration-Test vor Go-Live (Kategorie A/B)	100%
Kritische Findings vor Go-Live	0
Security-Requirements-Vollständigkeit	100%

### 67.8.2 8.2 Audit-Nachweise

- Security-Requirements-Dokumente
- Threat Models
- Security-Test-Berichte
- Security-Gateway-Genehmigungen
- DSFA (falls erforderlich)

## 67.9 9. Referenzen

### 67.9.1 Interne Dokumente

- 0680\_Policy\_Security\_in\_Projects.md
- 0390\_Richtlinie\_Secure\_SDLC\_Coding\_Review\_und\_Secrets.md

- 0470\_Richtlinie\_Third\_Party\_Risk\_Assessment\_und\_Cloud\_Controls.md
- 0570\_Richtlinie\_Datenschutz\_Anforderungen\_und\_Datenverarbeitung.md

### 67.9.2 Externe Standards

- ISO/IEC 27001:2022 Annex A.5.8 - Information security in project management
- NIST SP 800-64 - Security Considerations in the System Development Life Cycle
- OWASP SAMM - Software Assurance Maturity Model

---

**Genehmigt durch:** Thomas Weber, CISO

**Nächster Review:** {{ meta.document.next\_review }}

ewpage

# Chapter 68

## Anhang A: Annex A Control Mapping

**Dokumenttyp:** Anhang

**Version:** 1.0.0

**Datum:** {{ meta.document.date }}

**Klassifizierung:** internal

---

### 68.1 Zweck

Dieses Dokument stellt das vollständige Mapping der ISO/IEC 27001:2022 Annex A Kontrollen auf die implementierten Policies und Richtlinien des ISMS dar. Es dient als zentrale Referenz für die Compliance-Nachweisführung und zeigt auf, wie jede Annex A Kontrolle in der Organisation umgesetzt wird.

Das Mapping berücksichtigt die Änderungen aus Amendment 1:2024 und stellt sicher, dass alle 93 Kontrollen der aktuellen Annex A Version abgedeckt sind.

### 68.2 Geltungsbereich

**Organisation:** AdminSend GmbH

**ISMS Scope:** {{ meta.isms.scope }}

**Verantwortlich:** Thomas Weber (thomas.weber@adminsенд.de)

---

### 68.3 ISO/IEC 27001:2022 Annex A Struktur

Die Annex A Kontrollen sind in vier Hauptkategorien organisiert:

- **Organizational Controls (5.1-5.37):** 37 Kontrollen
- **People Controls (6.1-6.8):** 8 Kontrollen
- **Physical Controls (7.1-7.14):** 14 Kontrollen
- **Technological Controls (8.1-8.34):** 34 Kontrollen

**Gesamt:** 93 Kontrollen

---

## 68.4 Annex A Control Mapping

### 68.4.1 5. Organizational Controls

#### 68.4.1.1 5.1 Policies for Information Security

**Control Statement:** Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0010\_ISMS\_Informationssicherheitsleitlinie.md - Policy: 0200-0680 (Alle Topic-Specific Policies) - Prozess: 0050\_ISMS\_Dokumentenlenkung.md

**Verantwortlich:** Thomas Weber

**Nachweis:** Genehmigte und veröffentlichte Policies, Schulungsnachweise

---

#### 68.4.1.2 5.2 Information Security Roles and Responsibilities

**Control Statement:** Information security roles and responsibilities shall be defined and allocated according to the organization needs.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Dokument: 0040\_ISMS\_Governance\_Rollen\_und\_Verantwortlichkeiten.md - RACI-Matrizen in allen relevanten Policies

**Verantwortlich:** Thomas Weber

**Nachweis:** RACI-Matrizen, Stellenbeschreibungen, Organigramm

---

#### 68.4.1.3 5.3 Segregation of Duties

**Control Statement:** Conflicting duties and conflicting areas of responsibility shall be segregated.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0220\_Policy\_Zugriffssteuerung\_und\_Identitätsmanagement.md - Richtlinie: 0230\_Richtlinie\_IAM\_Joiner\_Mover\_Leaver\_und\_Zugriffsanträge.md

**Verantwortlich:** Thomas Weber

**Nachweis:** Berechtigungskonzept, Zugriffsreviews

---

#### 68.4.1.4 5.4 Management Responsibilities

**Control Statement:** Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0010\_ISMS\_Informationssicherheitsleitlinie.md - Dokument: 0120\_ISMS\_Schulung\_Awareness\_und\_Kompetenz.md

**Verantwortlich:** Management, Thomas Weber

**Nachweis:** Management-Commitment, Schulungsnachweise

---

#### 68.4.1.5 5.5 Contact with Authorities

**Control Statement:** The organization shall establish and maintain contact with relevant authorities.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Dokument: 0030\_ISMS\_Kontext\_und\_Interessierte\_Parteien.md - Policy: 0400\_Policy\_Incident\_Management.md

**Verantwortlich:** Thomas Weber

**Nachweis:** Kontaktlisten, Kommunikationsprotokolle

---

#### 68.4.1.6 5.6 Contact with Special Interest Groups

**Control Statement:** The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Dokument: 0030\_ISMS\_Kontext\_und\_Interessierte\_Parteien.md

**Verantwortlich:** Thomas Weber

**Nachweis:** Mitgliedschaften, Teilnahmebestätigungen

---

#### 68.4.1.7 5.7 Threat Intelligence

**Control Statement:** Information relating to information security threats shall be collected and analyzed to produce threat intelligence.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0340\_Policy\_Vulnerability\_und\_Patch\_Management.md - Richtlinie: 0350\_Richtlinie\_Vulnerability\_Scans\_Patching\_und\_Exploitation\_Response.md

**Verantwortlich:** Security Operations Team

**Nachweis:** Threat Intelligence Reports, Vulnerability Scans

---

#### 68.4.1.8 5.8 Information Security in Project Management

**Control Statement:** Information security shall be integrated into project management.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0680\_Policy\_Security\_in\_Projects.md - Richtlinie: 0690\_Richtlinie\_Sicherheits

**Verantwortlich:** Project Management Office, Thomas Weber

**Nachweis:** Projektdokumentation, Security Reviews

---

#### **68.4.1.9 5.9 Inventory of Information and Other Associated Assets**

**Control Statement:** An inventory of information and other associated assets, including owners, shall be developed and maintained.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0300\_Policy\_Asset\_Management.md - Richtlinie: 0310\_Richtlinie\_Asset\_Inven  
- Anhang: 0720\_Anhang\_Asset\_und\_Systeminventar\_Template.md

**Verantwortlich:** Asset Management Team

**Nachweis:** Asset Inventory, CMDB

---

#### **68.4.1.10 5.10 Acceptable Use of Information and Other Associated Assets**

**Control Statement:** Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0200\_Policy\_Akzeptable\_Nutzung\_IT.md - Richtlinie:  
0210\_Richtlinie\_Akzeptable\_Nutzung\_IT.md

**Verantwortlich:** Thomas Weber

**Nachweis:** Acceptable Use Policy, Mitarbeiterbestätigungen

---

#### **68.4.1.11 5.11 Return of Assets**

**Control Statement:** Personnel and other interested parties as appropriate shall return all of the organization's assets in their possession upon change or termination of their employment, contract or agreement.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0520\_Policy\_HR\_Security.md - Richtlinie: 0530\_Richtlinie\_HR\_Onboarding\_I

**Verantwortlich:** HR, IT Operations

**Nachweis:** Offboarding-Checklisten, Asset-Rückgabeprotokolle

---

#### **68.4.1.12 5.12 Classification of Information**

**Control Statement:** Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md  
- Richtlinie: 0290\_Richtlinie\_Datenklassifizierung\_Labeling\_und\_Handling.md

**Verantwortlich:** Data Owners, Thomas Weber

**Nachweis:** Klassifizierungsschema, gelabelte Dokumente

---

#### **68.4.1.13 5.13 Labelling of Information**

**Control Statement:** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Richtlinie: 0290\_Richtlinie\_Datenklassifizierung\_Labeling\_und\_Handling.md

**Verantwortlich:** Data Owners

**Nachweis:** Labelling-Richtlinien, gelabelte Assets

---

#### **68.4.1.14 5.14 Information Transfer**

**Control Statement:** Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0660\_Policy\_Informationsuebertragung\_und\_Kommunikation.md  
- Richtlinie: 0670\_Richtlinie\_Email\_Sharing\_und\_Zusammenarbeitstools.md

**Verantwortlich:** Thomas Weber

**Nachweis:** Transfer-Richtlinien, Verschlüsselungsnachweise

---

#### **68.4.1.15 5.15 Access Control**

**Control Statement:** Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0220\_Policy\_Zugriffssteuerung\_und\_Identitaetsmanagement.md  
- Richtlinie: 0230\_Richtlinie\_IAM\_Joiner\_Mover\_Leaver\_und\_Zugriffsantraege.md

**Verantwortlich:** IAM Team, Thomas Weber

**Nachweis:** Berechtigungskonzept, Access Reviews

---

#### **68.4.1.16 5.16 Identity Management**

**Control Statement:** The full life cycle of identities shall be managed.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0220\_Policy\_Zugriffssteuerung\_und\_Identitaetsmanagement.md  
- Richtlinie: 0230\_Richtlinie\_IAM\_Joiner\_Mover\_Leaver\_und\_Zugriffsantraege.md

**Verantwortlich:** IAM Team

**Nachweis:** Identity Lifecycle Prozesse, Joiner/Mover/Leaver Dokumentation

---

#### **68.4.1.17 5.17 Authentication Information**

**Control Statement:** Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0240\_Policy\_Authentisierung\_und\_Passwoerter.md - Richtlinie: 0250\_Richtlinie\_MFA\_Passwortregeln\_und\_Session\_Management.md

**Verantwortlich:** IAM Team

**Nachweis:** Passwort-Richtlinien, MFA-Implementierung

---

#### **68.4.1.18 5.18 Access Rights**

**Control Statement:** Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Richtlinie: 0230\_Richtlinie\_IAM\_Joiner\_Mover\_Leaver\_und\_Zugriffsantraege.md

**Verantwortlich:** IAM Team, Resource Owners

**Nachweis:** Access Request Workflows, Rezertifizierungsprotokolle

---

#### **68.4.1.19 5.19 Information Security in Supplier Relationships**

**Control Statement:** Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0460\_Policy\_Lieferanten\_und\_Cloud\_Sicherheit.md - Richtlinie: 0470\_Richtlinie\_Third\_Party\_Risk\_Assessment\_und\_Cloud\_Controls.md

**Verantwortlich:** Procurement, Thomas Weber

**Nachweis:** Supplier Security Assessments, Verträge

---

#### **68.4.1.20 5.20 Addressing Information Security within Supplier Agreements**

**Control Statement:** Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Richtlinie: 0470\_Richtlinie\_Third\_Party\_Risk\_Assessment\_und\_Cloud\_Controls.md

**Verantwortlich:** Procurement, Legal, Thomas Weber

**Nachweis:** Vertragsklauseln, SLAs

---

#### **68.4.1.21 5.21 Managing Information Security in the ICT Supply Chain**

**Control Statement:** Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Richtlinie: 0470\_Richtlinie\_Third\_Party\_Risk\_Assessment\_und\_Cloud\_Controls.md

**Verantwortlich:** Thomas Weber, IT Operations

**Nachweis:** Supply Chain Risk Assessments

---

#### **68.4.1.22 5.22 Monitoring, Review and Change Management of Supplier Services**

**Control Statement:** The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Richtlinie: 0470\_Richtlinie\_Third\_Party\_Risk\_Assessment\_und\_Cloud\_Controls.md

**Verantwortlich:** Supplier Management, Thomas Weber

**Nachweis:** Supplier Reviews, Performance Reports

---

#### **68.4.1.23 5.23 Information Security for Use of Cloud Services**

**Control Statement:** Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0460\_Policy\_Lieferanten\_und\_Cloud\_Sicherheit.md - Richtlinie: 0470\_Richtlinie\_Third\_Party\_Risk\_Assessment\_und\_Cloud\_Controls.md

**Verantwortlich:** Cloud Governance Team, Thomas Weber

**Nachweis:** Cloud Security Assessments, Cloud Contracts

---

#### **68.4.1.24 5.24 Information Security Incident Management Planning and Preparation**

**Control Statement:** The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0400\_Policy\_Incident\_Management.md - Richtlinie: 0410\_Richtlinie\_Incident\_Response\_und\_Major\_Incident\_Prozess.md

**Verantwortlich:** Incident Response Team, Thomas Weber

**Nachweis:** Incident Response Plan, Runbooks

---

#### **68.4.1.25 5.25 Assessment and Decision on Information Security Events**

**Control Statement:** The organization shall assess information security events and decide if they are to be categorized as information security incidents.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Richtlinie: 0410\_Richtlinie\_Incident\_Response\_und\_Major\_Incident\_Prozess.md

**Verantwortlich:** Incident Response Team

**Nachweis:** Event Classification Criteria, Incident Tickets

---

#### **68.4.1.26 5.26 Response to Information Security Incidents**

**Control Statement:** Information security incidents shall be responded to in accordance with the documented procedures.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Richtlinie: 0410\_Richtlinie\_Incident\_Response\_und\_Major\_Incident\_Prozess.md

**Verantwortlich:** Incident Response Team

**Nachweis:** Incident Response Dokumentation, Post-Mortems

---

#### **68.4.1.27 5.27 Learning from Information Security Incidents**

**Control Statement:** Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Richtlinie: 0410\_Richtlinie\_Incident\_Response\_und\_Major\_Incident\_Prozess.md  
- Dokument: 0160\_ISMS\_Kontinuierliche\_Verbesserung.md

**Verantwortlich:** Incident Response Team, Thomas Weber

**Nachweis:** Lessons Learned Dokumentation, Verbesserungsmaßnahmen

---

#### **68.4.1.28 5.28 Collection of Evidence**

**Control Statement:** The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Richtlinie: 0410\_Richtlinie\_Incident\_Response\_und\_Major\_Incident\_Prozess.md

**Verantwortlich:** Incident Response Team, Forensics Team

**Nachweis:** Forensics Procedures, Chain of Custody Dokumentation

---

#### **68.4.1.29 5.29 Information Security During Disruption**

**Control Statement:** The organization shall plan how to maintain information security at an appropriate level during disruption.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0440\_Policy\_Business\_Continuity\_ICT\_Readiness.md - Richtlinie: 0450\_Richtlinie\_ICT\_DR\_Schnittstellen\_zu\_BCM.md

**Verantwortlich:** BCM Team, Thomas Weber

**Nachweis:** Business Continuity Plans, DR Tests

---

#### **68.4.1.30 5.30 ICT Readiness for Business Continuity**

**Control Statement:** ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0440\_Policy\_Business\_Continuity\_ICT\_Readiness.md - Richtlinie: 0450\_Richtlinie\_ICT\_DR\_Schnittstellen\_zu\_BCM.md

**Verantwortlich:** IT Operations, BCM Team

**Nachweis:** DR Plans, BC Tests, RTO/RPO Dokumentation

---

#### **68.4.1.31 5.31 Legal, Statutory, Regulatory and Contractual Requirements**

**Control Statement:** Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Dokument: 0030\_ISMS\_Kontext\_und\_Interessierte\_Parteien.md - Policy: 0560\_Policy\_Datenschutz\_Schnittstellen.md

**Verantwortlich:** Legal, Compliance, Thomas Weber

**Nachweis:** Compliance Register, Legal Reviews

---

#### **68.4.1.32 5.32 Intellectual Property Rights**

**Control Statement:** The organization shall implement appropriate procedures to protect intellectual property rights.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0200\_Policy\_Akzeptable\_Nutzung\_IT.md - Richtlinie: 0290\_Richtlinie\_Datenklassifizierung\_Labeling\_und\_Handling.md

**Verantwortlich:** Legal, Thomas Weber

**Nachweis:** IP Protection Procedures, Lizenzmanagement

---

#### **68.4.1.33 5.33 Protection of Records**

**Control Statement:** Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0580\_Policy\_Aufbewahrung\_und\_Loeschung.md - Richtlinie: 0590\_Richtlinie\_Records\_Retention\_und\_Sichere\_Loeschung.md

**Verantwortlich:** Records Management, Thomas Weber

**Nachweis:** Records Retention Policy, Archivierungssysteme

---

#### **68.4.1.34 5.34 Privacy and Protection of PII**

**Control Statement:** The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0560\_Policy\_Datenschutz\_Schnittstellen.md - Richtlinie: 0570\_Richtlinie\_Datenschutz\_Anforderungen\_und\_Datenverarbeitung.md

**Verantwortlich:** Data Protection Officer, Thomas Weber

**Nachweis:** DSGVO Compliance, Privacy Impact Assessments

---

#### **68.4.1.35 5.35 Independent Review of Information Security**

**Control Statement:** The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Dokument: 0130\_ISMS\_Internes\_Auditprogramm.md

**Verantwortlich:** Internal Audit, Thomas Weber

**Nachweis:** Audit Reports, Audit Plans

---

#### **68.4.1.36 5.36 Compliance with Policies, Rules and Standards for Information Security**

**Control Statement:** Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Dokument: 0130\_ISMS\_Internes\_Auditprogramm.md - Dokument: 0140\_ISMS\_Management\_Review\_Template.md

**Verantwortlich:** Compliance Team, Thomas Weber

**Nachweis:** Compliance Reviews, Audit Findings

---

#### **68.4.1.37 5.37 Documented Operating Procedures**

**Control Statement:** Operating procedures for information processing facilities shall be documented and made available to personnel who need them.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Alle Richtlinien (0210-0690) - Dokument: 0050\_ISMS\_Dokumentenlenkung.md

**Verantwortlich:** IT Operations, Process Owners

**Nachweis:** Betriebsdokumentation, SOPs, Runbooks

---

### **68.4.2 6. People Controls**

#### **68.4.2.1 6.1 Screening**

**Control Statement:** Background verification checks on all candidates for employment shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0520\_Policy\_HR\_Security.md - Richtlinie: 0530\_Richtlinie\_HR\_Onboarding\_L

**Verantwortlich:** HR, Thomas Weber

**Nachweis:** Background Check Procedures, Screening Records

---

#### **68.4.2.2 6.2 Terms and Conditions of Employment**

**Control Statement:** The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0520\_Policy\_HR\_Security.md - Richtlinie: 0530\_Richtlinie\_HR\_Onboarding\_L

**Verantwortlich:** HR, Legal

**Nachweis:** Arbeitsverträge, NDA Templates

---

#### **68.4.2.3 6.3 Information Security Awareness, Education and Training**

**Control Statement:** Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Dokument: 0120\_ISMS\_Schulung\_Awareness\_und\_Kompetenz.md

**Verantwortlich:** Thomas Weber, HR

**Nachweis:** Schulungspläne, Teilnahmebestätigungen, Awareness Kampagnen

---

#### **68.4.2.4 6.4 Disciplinary Process**

**Control Statement:** A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0520\_Policy\_HR\_Security.md - Dokument: 0150\_ISMS\_Nichtkonformitaeten\_

**Verantwortlich:** HR, Management

**Nachweis:** Disziplinarverfahren, Dokumentierte Verstöße

---

#### **68.4.2.5 6.5 Responsibilities After Termination or Change of Employment**

**Control Statement:** Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0520\_Policy\_HR\_Security.md - Richtlinie: 0530\_Richtlinie\_HR\_Onboarding\_I

**Verantwortlich:** HR, IT Operations

**Nachweis:** Offboarding Checklisten, Exit Interviews

---

#### **68.4.2.6 6.6 Confidentiality or Non-Disclosure Agreements**

**Control Statement:** Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.

**Implementierungsstatus:** Implementiert  
**Umsetzung in ISMS:** - Policy: 0520\_Policy\_HR\_Security.md

**Verantwortlich:** Legal, HR

**Nachweis:** Unterzeichnete NDAs, Vertraulichkeitsvereinbarungen

---

#### **68.4.2.7 6.7 Remote Working**

**Control Statement:** Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0500\_Policy\_Mobile\_Device\_und\_Remote\_Work.md - Richtlinie: 0510\_Richtlinie\_MDM\_BringYourOwnDevice\_und\_Remote\_Access.md

**Verantwortlich:** IT Operations, Thomas Weber

**Nachweis:** Remote Work Policy, VPN Logs, Endpoint Security

---

#### **68.4.2.8 6.8 Information Security Event Reporting**

**Control Statement:** The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0400\_Policy\_Incident\_Management.md - Richtlinie: 0410\_Richtlinie\_Incident\_Response\_und\_Major\_Incident\_Prozess.md

**Verantwortlich:** All Personnel, Incident Response Team

**Nachweis:** Incident Reporting Channels, Event Reports

---

### **68.4.3 7. Physical Controls**

#### **68.4.3.1 7.1 Physical Security Perimeters**

**Control Statement:** Security perimeters shall be defined and used to protect areas that contain information and other associated assets.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0480\_Policy\_Physische\_Sicherheit.md - Richtlinie: 0490\_Richtlinie\_Zutritt\_Be

**Verantwortlich:** Facility Management, Thomas Weber

**Nachweis:** Sicherheitszonen, Zutrittskontrollsysteme

---

#### **68.4.3.2 7.2 Physical Entry**

**Control Statement:** Secure areas shall be protected by appropriate entry controls and access points.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Richtlinie: 0490\_Richtlinie\_Zutritt\_Besucher\_und\_Schutz\_von\_Equipment.md

**Verantwortlich:** Facility Management

**Nachweis:** Zutrittskontrollsysteem, Access Logs

---

#### **68.4.3.3 7.3 Securing Offices, Rooms and Facilities**

**Control Statement:** Physical security for offices, rooms and facilities shall be designed and implemented.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0480\_Policy\_Physische\_Sicherheit.md - Richtlinie: 0490\_Richtlinie\_Zutritt\_Be

**Verantwortlich:** Facility Management

**Nachweis:** Sicherheitskonzept Gebäude, Raumschutzmaßnahmen

---

#### **68.4.3.4 7.4 Physical Security Monitoring**

**Control Statement:** Premises shall be continuously monitored for unauthorized physical access.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Richtlinie: 0490\_Richtlinie\_Zutritt\_Besucher\_und\_Schutz\_von\_Equipment.md

**Verantwortlich:** Security Operations, Facility Management

**Nachweis:** Videoüberwachung, Alarmsysteme, Security Logs

---

#### **68.4.3.5 7.5 Protecting Against Physical and Environmental Threats**

**Control Statement:** Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0480\_Policy\_Physische\_Sicherheit.md - Policy: 0440\_Policy\_Business\_Continuity\_ICT\_Readiness.md

**Verantwortlich:** Facility Management, BCM Team

**Nachweis:** Umweltschutzmaßnahmen, Brandschutz, Klimatisierung

---

#### **68.4.3.6 7.6 Working in Secure Areas**

**Control Statement:** Security measures for working in secure areas shall be designed and implemented.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Richtlinie: 0490\_Richtlinie\_Zutritt\_Besucher\_und\_Schutz\_von\_Equipment.md

**Verantwortlich:** Facility Management, Thomas Weber  
**Nachweis:** Clean Desk Policy, Secure Area Procedures

---

#### 68.4.3.7 7.7 Clear Desk and Clear Screen

**Control Statement:** Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0480\_Policy\_Physische\_Sicherheit.md - Policy: 0200\_Policy\_Akzeptable\_Nutzung\_IT.md

**Verantwortlich:** All Personnel, Management

**Nachweis:** Clear Desk Policy, Awareness Training

---

#### 68.4.3.8 7.8 Equipment Siting and Protection

**Control Statement:** Equipment shall be sited securely and protected.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Richtlinie: 0490\_Richtlinie\_Zutritt\_Besucher\_und\_Schutz\_von\_Equipment.md

**Verantwortlich:** IT Operations, Facility Management

**Nachweis:** Serverraum-Sicherheit, Equipment Protection Measures

---

#### 68.4.3.9 7.9 Security of Assets Off-Premises

**Control Statement:** Off-site assets shall be protected.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0500\_Policy\_Mobile\_Device\_und\_Remote\_Work.md - Richtlinie: 0510\_Richtlinie\_MDM\_BringYourOwnDevice\_und\_Remote\_Access.md

**Verantwortlich:** IT Operations, Thomas Weber

**Nachweis:** Mobile Device Management, Encryption Policies

---

#### 68.4.3.10 7.10 Storage Media

**Control Statement:** Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0300\_Policy\_Asset\_Management.md - Richtlinie: 0310\_Richtlinie\_Asset\_Inven

**Verantwortlich:** IT Operations

**Nachweis:** Media Handling Procedures, Disposal Records

---

#### **68.4.3.11 7.11 Supporting Utilities**

**Control Statement:** Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0440\_Policy\_Business\_Continuity ICT Readiness.md - Richtlinie: 0450\_Richtlinie ICT DR Schnittstellen zu BCM.md

**Verantwortlich:** IT Operations, Facility Management

**Nachweis:** USV-Systeme, Redundante Stromversorgung

---

#### **68.4.3.12 7.12 Cabling Security**

**Control Statement:** Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0480\_Policy\_Physische\_Sicherheit.md - Policy: 0600\_Policy\_Netzwerksicherheit.md

**Verantwortlich:** IT Operations, Facility Management

**Nachweis:** Kabelschutzmaßnahmen, Netzwerkdokumentation

---

#### **68.4.3.13 7.13 Equipment Maintenance**

**Control Statement:** Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0300\_Policy\_Asset\_Management.md - Richtlinie: 0310\_Richtlinie\_Asset\_Inv...

**Verantwortlich:** IT Operations

**Nachweis:** Wartungspläne, Maintenance Records

---

#### **68.4.3.14 7.14 Secure Disposal or Re-use of Equipment**

**Control Statement:** Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Richtlinie: 0310\_Richtlinie\_Asset\_Inventory\_Tagging\_und\_Entsorgung.md - Policy: 0580\_Policy\_Aufbewahrung\_und\_Loeschung.md

**Verantwortlich:** IT Operations

**Nachweis:** Secure Disposal Procedures, Wiping Certificates

---

## **68.4.4 8. Technological Controls**

### **68.4.4.1 8.1 User Endpoint Devices**

**Control Statement:** Information stored on, processed by or accessible via user endpoint devices shall be protected.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0620\_Policy\_Endpoint\_Security.md - Richtlinie: 0630\_Richtlinie\_EDR\_AV\_H

**Verantwortlich:** IT Operations, Thomas Weber

**Nachweis:** Endpoint Protection, Device Compliance Policies

---

### **68.4.4.2 8.2 Privileged Access Rights**

**Control Statement:** The allocation and use of privileged access rights shall be restricted and managed.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0220\_Policy\_Zugriffssteuerung\_und\_Identitaetsmanagement.md  
- Richtlinie: 0230\_Richtlinie\_IAM\_Joiner\_Mover\_Leaver\_und\_Zugriffsantraege.md

**Verantwortlich:** IAM Team, Thomas Weber

**Nachweis:** Privileged Access Management, PAM Logs

---

### **68.4.4.3 8.3 Information Access Restriction**

**Control Statement:** Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0220\_Policy\_Zugriffssteuerung\_und\_Identitaetsmanagement.md  
- Richtlinie: 0230\_Richtlinie\_IAM\_Joiner\_Mover\_Leaver\_und\_Zugriffsantraege.md

**Verantwortlich:** IAM Team, Data Owners

**Nachweis:** Access Control Lists, Authorization Policies

---

### **68.4.4.4 8.4 Access to Source Code**

**Control Statement:** Read and write access to source code, development tools and software libraries shall be appropriately managed.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0380\_Policy\_Secure\_Development.md - Richtlinie: 0390\_Richtlinie\_Secure\_SD

**Verantwortlich:** Development Team, Thomas Weber

**Nachweis:** Source Code Access Controls, Git Permissions

---

#### **68.4.4.5 8.5 Secure Authentication**

**Control Statement:** Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0240\_Policy\_Authentisierung\_und\_Passwoerter.md - Richtlinie: 0250\_Richtlinie\_MFA\_Passwortregeln\_und\_Session\_Management.md

**Verantwortlich:** IAM Team

**Nachweis:** MFA Implementation, Authentication Logs

---

#### **68.4.4.6 8.6 Capacity Management**

**Control Statement:** The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0320\_PolicyLogging\_und\_Monitoring.md - Richtlinie: 0330\_RichtlinieLogging\_SIEM\_und\_Audit\_Trails.md

**Verantwortlich:** IT Operations

**Nachweis:** Capacity Monitoring, Performance Reports

---

#### **68.4.4.7 8.7 Protection Against Malware**

**Control Statement:** Protection against malware shall be implemented and supported by appropriate user awareness.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0620\_Policy\_Endpoint\_Security.md - Richtlinie: 0630\_Richtlinie\_EDR\_AV\_H

**Verantwortlich:** IT Operations, Thomas Weber

**Nachweis:** Antivirus/EDR Deployment, Malware Detection Logs

---

#### **68.4.4.8 8.8 Management of Technical Vulnerabilities**

**Control Statement:** Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0340\_Policy\_Vulnerability\_und\_Patch\_Management.md - Richtlinie: 0350\_Richtlinie\_Vulnerability\_Scans\_Patching\_und\_Explotation\_Response.md

**Verantwortlich:** Security Operations, IT Operations

**Nachweis:** Vulnerability Scans, Patch Management Reports

---

#### **68.4.4.9 8.9 Configuration Management**

**Control Statement:** Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0540\_Policy\_Konfiguration\_und\_Hardening.md - Richtlinie: 0550\_Richtlinie\_Sicherheitsbaselines\_Hardening\_und\_Konfig\_Aenderungen.md

**Verantwortlich:** IT Operations, Thomas Weber

**Nachweis:** Configuration Management Database, Baseline Configurations

---

#### **68.4.4.10 8.10 Information Deletion**

**Control Statement:** Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0580\_Policy\_Aufbewahrung\_und\_Loeschung.md - Richtlinie: 0590\_Richtlinie\_Records\_Retention\_und\_Sichere\_Loeschung.md

**Verantwortlich:** Data Owners, IT Operations

**Nachweis:** Data Retention Policy, Deletion Logs

---

#### **68.4.4.11 8.11 Data Masking**

**Control Statement:** Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0560\_Policy\_Datenschutz\_Schnittstellen.md - Richtlinie: 0570\_Richtlinie\_Datenschutz\_Anforderungen\_und\_Datenverarbeitung.md

**Verantwortlich:** Development Team, Data Protection Officer

**Nachweis:** Data Masking Procedures, Test Data Management

---

#### **68.4.4.12 8.12 Data Leakage Prevention**

**Control Statement:** Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0280\_Policy\_Datenklassifizierung\_und\_Informationshandling.md - Richtlinie: 0290\_Richtlinie\_Datenklassifizierung\_Labeling\_und\_Handling.md

**Verantwortlich:** Security Operations, Thomas Weber  
**Nachweis:** DLP Implementation, DLP Alerts

---

#### 68.4.4.13 8.13 Information Backup

**Control Statement:** Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0420\_Policy\_Backup\_und\_Wiederherstellung.md - Richtlinie: 0430\_Richtlinie\_Backup\_Restore\_und\_Regelmaessige\_Tests.md

**Verantwortlich:** IT Operations

**Nachweis:** Backup Policies, Restore Tests, Backup Logs

---

#### 68.4.4.14 8.14 Redundancy of Information Processing Facilities

**Control Statement:** Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0440\_Policy\_Business\_Continuity ICT Readiness.md - Richtlinie: 0450\_Richtlinie ICT DR Schnittstellen zu BCM.md

**Verantwortlich:** IT Operations, IT Architecture

**Nachweis:** High Availability Designs, Redundancy Documentation

---

#### 68.4.4.15 8.15 Logging

**Control Statement:** Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analyzed.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0320\_PolicyLogging\_und\_Monitoring.md - Richtlinie: 0330\_Richtlinie Logging SIEM und Audit Trails.md

**Verantwortlich:** IT Operations, Security Operations

**Nachweis:** Logging Standards, SIEM Implementation, Log Retention

---

#### 68.4.4.16 8.16 Monitoring Activities

**Control Statement:** Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0320\_PolicyLogging\_und\_Monitoring.md - Richtlinie: 0330\_Richtlinie Logging SIEM und Audit Trails.md

**Verantwortlich:** Security Operations

**Nachweis:** SIEM Use Cases, Monitoring Dashboards, Alerts

---

#### **68.4.4.17 8.17 Clock Synchronization**

**Control Statement:** The clocks of information processing systems used by the organization shall be synchronized to approved time sources.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0540\_Policy\_Konfiguration\_und\_Hardening.md - Richtlinie: 0550\_Richtlinie\_Sicherheitsbaselines\_Hardening\_und\_Konfig\_Aenderungen.md

**Verantwortlich:** IT Operations

**Nachweis:** NTP Configuration, Time Synchronization Logs

---

#### **68.4.4.18 8.18 Use of Privileged Utility Programs**

**Control Statement:** The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0220\_Policy\_Zugriffssteuerung\_und\_Identitaetsmanagement.md - Richtlinie: 0230\_Richtlinie\_IAM\_Joiner\_Mover\_Leaver\_und\_Zugriffsantraege.md

**Verantwortlich:** IT Operations, Thomas Weber

**Nachweis:** Privileged Access Controls, Utility Program Restrictions

---

#### **68.4.4.19 8.19 Installation of Software on Operational Systems**

**Control Statement:** Procedures and measures shall be implemented to securely manage software installation on operational systems.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0360\_Policy\_Change\_und\_Release\_Management.md - Richtlinie: 0370\_Richtlinie\_Change\_Management\_mit\_Sicherheitsfreigaben.md

**Verantwortlich:** IT Operations, Change Management

**Nachweis:** Software Installation Procedures, Change Records

---

#### **68.4.4.20 8.20 Networks Security**

**Control Statement:** Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0600\_Policy\_Netzwerksicherheit.md - Richtlinie: 0610\_Richtlinie\_Segmentierung

**Verantwortlich:** Network Team, Thomas Weber  
**Nachweis:** Network Security Architecture, Firewall Rules

---

#### 68.4.4.21 8.21 Security of Network Services

**Control Statement:** Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0600\_Policy\_Netzwerksicherheit.md - Richtlinie: 0610\_Richtlinie\_Segmentierung\_Firewalling\_und\_Network\_Access\_Control.md

**Verantwortlich:** Network Team

**Nachweis:** Network Service SLAs, Security Monitoring

---

#### 68.4.4.22 8.22 Segregation of Networks

**Control Statement:** Groups of information services, users and information systems shall be segregated in the organization's networks.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Richtlinie: 0610\_Richtlinie\_Segmentierung\_Firewalling\_und\_Network\_Access\_Control.md

**Verantwortlich:** Network Team, Thomas Weber

**Nachweis:** Network Segmentation Design, VLAN Configuration

---

#### 68.4.4.23 8.23 Web Filtering

**Control Statement:** Access to external websites shall be managed to reduce exposure to malicious content.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0600\_Policy\_Netzwerksicherheit.md - Policy: 0620\_Policy\_Endpoint\_Security.md

**Verantwortlich:** Security Operations, IT Operations

**Nachweis:** Web Filtering Solution, Blocked Content Logs

---

#### 68.4.4.24 8.24 Use of Cryptography

**Control Statement:** Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0260\_Policy\_Kryptografie\_und\_Schluesselmanagement.md - Richtlinie: 0270\_Richtlinie\_Key\_Management\_und\_Verschlusselfung.md

**Verantwortlich:** Thomas Weber, IT Operations

**Nachweis:** Cryptography Policy, Key Management Procedures

---

#### 68.4.4.25 8.25 Secure Development Life Cycle

**Control Statement:** Rules for the secure development of software and systems shall be established and applied.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0380\_Policy\_Secure\_Development.md - Richtlinie: 0390\_Richtlinie\_Secure\_SD

**Verantwortlich:** Development Team, Thomas Weber

**Nachweis:** Secure SDLC Procedures, Code Review Records

---

#### 68.4.4.26 8.26 Application Security Requirements

**Control Statement:** Information security requirements shall be identified, specified and approved when developing or acquiring applications.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0380\_Policy\_Secure\_Development.md - Richtlinie: 0390\_Richtlinie\_Secure\_SD

**Verantwortlich:** Development Team, Security Architecture

**Nachweis:** Security Requirements Specifications, Threat Models

---

#### 68.4.4.27 8.27 Secure System Architecture and Engineering Principles

**Control Statement:** Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0380\_Policy\_Secure\_Development.md - Richtlinie: 0390\_Richtlinie\_Secure\_SD

**Verantwortlich:** Security Architecture, Development Team

**Nachweis:** Secure Architecture Principles, Design Reviews

---

#### 68.4.4.28 8.28 Secure Coding

**Control Statement:** Secure coding principles shall be applied to software development.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Richtlinie: 0390\_Richtlinie\_Secure\_SDLC\_Coding\_Review\_und\_Secrets.md

**Verantwortlich:** Development Team

**Nachweis:** Secure Coding Guidelines, SAST/DAST Results

---

#### **68.4.4.29 8.29 Security Testing in Development and Acceptance**

**Control Statement:** Security testing processes shall be defined and implemented in the development life cycle.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Richtlinie: 0390\_Richtlinie\_Secure\_SDLC\_Coding\_Review\_und\_Secrets.md

**Verantwortlich:** Development Team, Security Team

**Nachweis:** Security Test Plans, Penetration Test Reports

---

#### **68.4.4.30 8.30 Outsourced Development**

**Control Statement:** The organization shall direct, monitor and review the activities related to outsourced system development.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0460\_Policy\_Lieferanten\_und\_Cloud\_Sicherheit.md - Richtlinie: 0470\_Richtlinie\_Third\_Party\_Risk\_Assessment\_und\_Cloud\_Controls.md

**Verantwortlich:** Development Team, Thomas Weber

**Nachweis:** Supplier Contracts, Development Oversight Records

---

#### **68.4.4.31 8.31 Separation of Development, Test and Production Environments**

**Control Statement:** Development, testing and production environments shall be separated and secured.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0380\_Policy\_Secure\_Development.md - Richtlinie: 0390\_Richtlinie\_Secure\_SD

**Verantwortlich:** Development Team, IT Operations

**Nachweis:** Environment Separation, Access Controls per Environment

---

#### **68.4.4.32 8.32 Change Management**

**Control Statement:** Changes to information processing facilities and information systems shall be subject to change management procedures.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0360\_Policy\_Change\_und\_Release\_Management.md - Richtlinie: 0370\_Richtlinie\_Change\_Management\_mit\_Sicherheitsfreigaben.md

**Verantwortlich:** Change Management, IT Operations

**Nachweis:** Change Management Process, Change Records

---

#### **68.4.4.33 8.33 Test Information**

**Control Statement:** Test information shall be appropriately selected, protected and managed.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Policy: 0560\_Policy\_Datenschutz\_Schnittstellen.md - Richtlinie: 0570\_Richtlinie\_Datenschutz\_Anforderungen\_und\_Datenverarbeitung.md

**Verantwortlich:** Development Team, Data Protection Officer

**Nachweis:** Test Data Management, Data Masking Procedures

---

#### **68.4.4.34 8.34 Protection of Information Systems During Audit Testing**

**Control Statement:** Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.

**Implementierungsstatus:** Implementiert

**Umsetzung in ISMS:** - Dokument: 0130\_ISMS\_Internes\_Auditprogramm.md

**Verantwortlich:** Internal Audit, IT Operations

**Nachweis:** Audit Plans, Test Approvals, Audit Protocols

---

### **68.5 Amendment 1:2024 Änderungen**

**Hinweis:** ISO/IEC 27001:2022 Amendment 1:2024 führt keine neuen Kontrollen ein, sondern präzisiert bestehende Kontrollen und aktualisiert Referenzen. Die wichtigsten Änderungen betreffen:

- **5.7 Threat Intelligence:** Erweiterte Anforderungen an Threat Intelligence Prozesse
- **5.23 Information Security for Use of Cloud Services:** Aktualisierte Cloud Security Anforderungen
- **8.11 Data Masking:** Neue Kontrolle für Datenmaskierung (bereits in 2022 enthalten)
- **8.12 Data Leakage Prevention:** Neue Kontrolle für DLP (bereits in 2022 enthalten)

Alle Änderungen sind in diesem Mapping bereits berücksichtigt.

---

### **68.6 Zusammenfassung**

#### **68.6.1 Implementierungsstatus Übersicht**

Kategorie	Anzahl Kontrollen	Implementiert	Teilweise	Nicht implementiert
Organizational Controls (5.x)	37	0	0	

Kategorie	Anzahl Kontrollen	Implementiert	Teilweise	Nicht implementiert
People Controls (6.x)	8	8	0	0
Physical Controls (7.x)	14	14	0	0
Technological Controls (8.x)	34	34	0	0
<b>Gesamt</b>	<b>93</b>	<b>93</b>	<b>0</b>	<b>0</b>

**Implementierungsgrad:** 100%

---

## 68.7 Verwendung dieses Mappings

Dieses Mapping dient als:

1. **Compliance-Nachweis:** Zeigt auf, wie jede Annex A Kontrolle umgesetzt wird
2. **Audit-Vorbereitung:** Ermöglicht schnelle Identifikation relevanter Dokumente
3. **Gap-Analyse:** Identifiziert fehlende oder unvollständige Implementierungen
4. **Wartung:** Unterstützt bei der Aktualisierung des ISMS

**Aktualisierung:** Dieses Dokument sollte bei jeder Änderung an Policies, Richtlinien oder Kontrollen aktualisiert werden.

---

## 68.8 Referenzen

- ISO/IEC 27001:2022 Information Security Management Systems - Requirements
  - ISO/IEC 27001:2022/Amd 1:2024 Amendment 1
  - ISO/IEC 27002:2022 Information Security Controls
  - Statement of Applicability (SoA): 0100\_ISMS\_Statement\_of\_Applicability\_SoA\_Template.md
- 

**Dokumentverantwortlicher:** Thomas Weber

**Genehmigt durch:** {{ meta.management.name }}

**Nächste Überprüfung:** {{ meta.document.next\_review }}

ewpage

# Chapter 69

## Anhang B: Asset- und Systeminventar

**Dokumenttyp:** Anhang

**Version:** 1.0.0

**Datum:** {{ meta.document.date }}

**Klassifizierung:** internal

---

### 69.1 Zweck

Dieses Dokument stellt das zentrale Asset- und Systeminventar der Organisation dar. Es erfüllt die Anforderungen von ISO/IEC 27001:2022 Annex A 5.9 (Inventory of Information and Other Associated Assets) und dient als Grundlage für:

- Asset Management und Lifecycle-Verwaltung
- Risikobewertung und Schutzbedarfsfeststellung
- Incident Response und Business Continuity Planning
- Compliance-Nachweisführung und Audits

Das Inventar wird kontinuierlich gepflegt und mindestens quartalsweise überprüft.

### 69.2 Geltungsbereich

**Organisation:** AdminSend GmbH

**ISMS Scope:** {{ meta.isms.scope }}

**Verantwortlich:** Asset Management Team, Thomas Weber

---

### 69.3 Asset-Kategorien

Das Inventar umfasst folgende Asset-Kategorien:

1. **Hardware Assets:** Server, Netzwerkgeräte, Endpoints, Storage
2. **Software Assets:** Betriebssysteme, Anwendungen, Lizenzen
3. **Daten Assets:** Datenbanken, Dateisysteme, Repositories

4. **Netzwerk Assets:** VLANs, Subnetze, Verbindungen
  5. **Cloud Assets:** Cloud Services, SaaS-Anwendungen
  6. **Physische Assets:** Räume, Infrastruktur, Dokumentation
- 

## 69.4 Asset-Klassifizierung

Jedes Asset wird nach folgenden Kriterien klassifiziert:

### 69.4.1 Schutzbedarf (Confidentiality, Integrity, Availability)

Stufe	Beschreibung	Beispiel
<b>Hoch</b>	Kritisch für Geschäftsbetrieb, hoher Schaden bei Kompromittierung	Produktionsdatenbanken, Core Banking Systems
<b>Mittel</b>	Wichtig für Geschäftsbetrieb, mittlerer Schaden bei Kompromittierung	Interne Anwendungen, Entwicklungssysteme
<b>Niedrig</b>	Unkritisch, geringer Schaden bei Kompromittierung	Test-Systeme, öffentliche Informationen

### 69.4.2 Kritikalität

Stufe	RTO	RPO	Beschreibung
<b>Tier 1</b>	< 4h	< 1h	Geschäftskritisch, sofortige Wiederherstellung erforderlich
<b>Tier 2</b>	< 24h	< 4h	Wichtig, Wiederherstellung innerhalb eines Arbeitstages
<b>Tier 3</b>	< 72h	< 24h	Standard, Wiederherstellung innerhalb von 3 Tagen
<b>Tier 4</b>	> 72h	> 24h	Unkritisch, keine zeitkritische Wiederherstellung

## 69.5 Hardware Assets

### 69.5.1 Server

Asset-ID	Hostname	Typ	Standort	Owner	Schutzbedarf (C/I/A)		Kritikalität	Status	
					C	I			
SRV-001	{{ net- box.device.p }} Physical Server name@ {{ net- box.device.p }} {{ net- box.device.p }}	Physical Server	IT Operations	IT Operations	Hoch	Hoch	Hoch	Tier 1	Produktiv

Asset-ID	Hostname	Typ	Standort	Owner	Schutzbedarf (C/I/A)	Kritikalität	Status
SRV-002	<code>{} net-Physical{ net- box.device.boxname}IT</code>				Hoch/Hoch/Mittel	Tier 2	Produktiv
[TODO]	<code>[TODO: Host- name] [TODO: Typ]</code>	<code>[TODO: Standort]</code>	<code>[TODO: Owner]</code>		<code>[TODO: C/I/A]</code>	<code>[TODO: Tier]</code>	<code>[TODO: Status]</code>

**Hinweis:** Vollständige Server-Liste aus NetBox/CMDB importieren.

---

### 69.5.2 Netzwerkgeräte

Asset-ID	Hostname	Typ	Standort	Owner	Schutzbedarf (C/I/A)	Kritikalität	Status
NET-001	<code>{} net-Core{ net- box.device.switch.sitenameTeam}</code>				Network Mittel/Hoch/Hoch	Tier 1	Produktiv
NET-002	<code>{} net-Firewall{ net- box.device.firewall.homeSite.nameTeam}</code>				Hoch/Hoch/Hoch	Tier 1	Produktiv
[TODO]	<code>[TODO: Host- name]</code>	<code>[TODO: Typ]</code>	<code>[TODO: Standort]</code>	<code>[TODO: Owner]</code>	<code>[TODO: C/I/A]</code>	<code>[TODO: Tier]</code>	<code>[TODO: Status]</code>

**Hinweis:** Vollständige Netzwerkgeräte-Liste aus NetBox importieren.

---

### 69.5.3 Endpoints

Asset-ID	Hostname	Typ	Benutzer	Owner	Schutzbedarf (C/I/A)	Status
WS-001	<code>{} Laptop</code>	Thomas		IT Operations	Hoch/Mittel/Mittel	Produktiv
	<code>meta.ciso.workstation</code>	Weber				
[TODO]	<code>[TODO: Hostname]</code>	<code>[TODO: Typ]</code>	<code>[TODO: Benutzer]</code>	<code>[TODO: Owner]</code>	<code>[TODO: C/I/A]</code>	<code>[TODO: Status]</code>

**Hinweis:** Endpoint-Inventar aus MDM/Endpoint Management System importieren.

---

## 69.5.4 Storage-Systeme

Asset-ID	Name	Typ	Kapazität	Standort	Owner	Schutzbedarf (C/I/A)	Kritikalität
STO-001	{} net- box.device.storage }	SAN	[TODO: Kapaz- ität]	{ net- box.site.name }	IT Operations	Hoch/Hoch/Hoch	Tier 1
[TODO]	[TODO:[TODO: Name] [TODO: Typ]	[TODO: Kapaz- ität]	[TODO: Standort]	[TODO: Owner]	[TODO: C/I/A]	[TODO: Tier]	

## 69.6 Software Assets

### 69.6.1 Betriebssysteme

Asset-ID	Name	Version	Lizenztyp	Anzahl Lizenzen	Owner	Kritikalität
OS-001	Windows Server	2022	Volume License	[TODO: Anzahl]	IT Operations	Tier 1
OS-002	Red Hat Enterprise Linux	9.x	Subscription	[TODO: Anzahl]	IT Operations	Tier 1
OS-003	Ubuntu Server	22.04 LTS	Open Source	Unbegrenzt	IT Operations	Tier 2
[TODO]	[TODO: [TODO: Name] [TODO: Version]	[TODO: Lizenztyp]	[TODO: Anzahl]	[TODO: Owner]	[TODO: [TODO: Tier]	

### 69.6.2 Geschäftsanwendungen

Asset-ID	Name	Version	Vendor	Lizenztyp	Owner	Schutzbedarf (C/I/A)	Kritikalität
APP-001	[TODO:[TODO: ERP Version]	[TODO: Sys- tem]	[TODO: Ven- dor]	[TODO: Lizenz- typ]	[TODO: Owner]	Business Hoch/Hoch/Hoch	Tier 1
APP-002	[TODO:[TODO: CRM Version]	[TODO: Sys- tem]	[TODO: Ven- dor]	[TODO: Lizenz- typ]	Sales	Hoch/Mittel/Mittel	Tier 2

Asset-ID	Name	Version	Vendor	Lizenztyp	Owner	Schutzbedarf		Kritikalität
						(C/I/A)		
[TODO]	[TODO:[TODO: Name] Version]		[TODO: Ven- dor]	[TODO: Lizenz- typ]	[TODO: Owner]	[TODO: [TODO: C/I/A]		[TODO: Tier]

### 69.6.3 Sicherheitssoftware

Asset-ID	Name	Version	Typ	Abdeckung	Owner	Kritikalität
SEC-001	[TODO: EDR Solu- tion]	[TODO: Version]	Endpoint Detec- tion & Re- sponse	Alle Endpoints	Security Team	Tier 1
SEC-002	[TODO: SIEM]	[TODO: Version]	Security Infor- ma- tion & Event Man- age- ment	Alle Systeme	Security Team	Tier 1
SEC-003	[TODO: Fire- wall]	[TODO: Version]	Next- Gen Fire- wall	Perimeter	Security Team	Tier 1
[TODO]	[TODO: Name]	[TODO: Version]	[TODO: Typ]	[TODO: Abdeckung]	[TODO: Owner]	[TODO: Tier]

## 69.7 Daten Assets

### 69.7.1 Datenbanken

Asset-ID	Name	Typ	Version	Server	Owner	Schutzbedarf		Backup
						(C/I/A)		
DB-001	[TODO:[TODO: Produkt- DB]	[TODO: Test- DB]	[TODO: Version]	SRV- 001	DBA	Hoch/Hoch/Hoch	Tier 1	Täglich
DB-002	[TODO:[TODO: Test- DB]	[TODO: Typ]	[TODO: Version]	[TODO: Server]	DBA	Niedrig/Mittel/Niedrig	Tier 3	Wöchentlich

Asset-ID	Name	Typ	Version	Server	Owner	Schutzbedarf		Kritikalität	Backup
						(C/I/A)			
[TODO]	[TODO:[TODO:[TODO:			[TODO:	[TODO:	[TODO:	C/I/A]	[TODO:	[TODO:
	Name]	Typ]	Version]	Server]	Owner]			Tier]	Backup]

### 69.7.2 Dateisysteme und Shares

Asset-ID	Name	Typ	Pfad	Server	Owner	Schutzbedarf (C/I/A)	Backup
FS-001	[TODO: SMB Abteilung Share]	[TODO: Share]	[TODO: Pfad]	[TODO: Server]	IT Opera- tions	Mittel/Mittel/Mittel	Täglich
FS-002	[TODO: SMB Projekt- Share]	[TODO: Share]	[TODO: Pfad]	[TODO: Server]	Project Man- age- ment	Hoch/Mittel/Mittel	Täglich
[TODO]	[TODO: [TODO:[TODO: [TODO:			[TODO:	[TODO:	C/I/A]	[TODO:
	Name]	Typ]	Pfad]	Server]	Owner]		Backup]

### 69.7.3 Code Repositories

Asset-ID	Name	Typ	URL	Owner	Schutzbedarf (C/I/A)	Backup
REPO-001	[TODO: Git Main Reposi- tory]	[TODO: URL]	[TODO: Developmen URL]	Hoch/Hoch/Mittel Team		Täglich
[TODO]	[TODO: [TODO: [TODO: [TODO:			[TODO: Owner]	C/I/A]	[TODO: Backup]
	Name]	Typ]	URL]			

## 69.8 Netzwerk Assets

### 69.8.1 VLANs

VLAN-ID	Name	Subnet	Zweck	Sicherheitszone	Owner
{} net- box.vlan.manage- {} }{	{} net- box.vlan.manage- {} }{	{} net- box.vlan.manage- {} }{	Management	Restricted	Network Team

VLAN-ID	Name	Subnet	Zweck	Sicherheitszone	Owner
<code>{} net-box.vlan.product</code>	<code>{} net-box.wlan.production</code>	<code>{} net-box.wlan.production</code>	Production	Internal	Network Team
<code>}</code>	<code>}</code>	<code>}</code>			

**Hinweis:** Vollständige VLAN-Liste aus NetBox importieren.

---

### 69.8.2 Externe Verbindungen

Verbindungs-ID	Typ	Provider	Bandbreite	Zweck	Owner	Kritikalität
WAN-001	Internet	[TODO: Provider]	[TODO: Bandbreite]	Internet	Network	Tier 1
WAN-002	MPLS	[TODO: Provider]	[TODO: Bandbreite]	Access	Team	
[TODO]	[TODO: Typ]	[TODO: Provider]	[TODO: Bandbreite]	Site-to-Site	Network	Tier 1

---

## 69.9 Cloud Assets

### 69.9.1 Cloud Services (IaaS/PaaS)

Asset-ID	Service Name	Provider	Typ	Region	Owner	Schutzbedarf (C/I/A)	Kritikalität
CLOUD-001	[TODO: VM Instances]	[TODO: AWS/Azure/GCP]	IaaS	[TODO: Region]	Cloud Team	Hoch/Hoch/Hoch	Tier 1
CLOUD-002	[TODO: Database Service]	[TODO: Provider]	PaaS	[TODO: Region]	DBA Team	Hoch/Hoch/Hoch	Tier 1
[TODO]	[TODO: Service]	[TODO: Provider]	[TODO: Typ]	[TODO: Region]	[TODO: Owner]	[TODO: C/I/A]	[TODO: Tier]

---

### 69.9.2 SaaS-Anwendungen

Asset-ID	Service Name	Provider	Zweck	Benutzeranzahl	Owner	Schutzbedarf (C/I/A)
SAAS-001	Microsoft 365	Microsoft	Productivität	[TODO: Anzahl]	IT Operations	Hoch/Mittel/Hoch
SAAS-002	[TODO: CRM SaaS]	[TODO: Provider]	Customer Management	[TODO: Anzahl]	Sales	Hoch/Mittel/Mittel
[TODO]	[TODO: Service]	[TODO: Provider]	[TODO: Zweck]	[TODO: Anzahl]	[TODO: Owner]	[TODO: C/I/A]

## 69.10 Physische Assets

### 69.10.1 Standorte und Räume

Standort-ID	Name	Adresse	Typ	Sicherheitsstufe	Owner
SITE-001	<code>{} net-box.site.name</code>	<code>{} netbox.site.address</code>	Hauptstandort	Hoch	Facility Management
SITE-002	[TODO: Zweigstelle]	[TODO: Adresse]	Zweigstelle	Mittel	Facility Management
[TODO]	[TODO: Name]	[TODO: Adresse]	[TODO: Typ]	[TODO: Sicherheit]	[TODO: Owner]

### 69.10.2 Serverräume und Rechenzentren

Raum-ID	Name	Standort	Typ	Größe	Klimatisierung	Brandschutz	Zutrittskontrolle
ROOM-001	Serverraum 1	SITE-001	Serverraum	[TODO: m <sup>2</sup> ]	[TODO: Redundant Klima]	FM-200	Biometrisch
[TODO]	[TODO: Name]	[TODO: Standort]	[TODO: Typ]	[TODO: Größe]	[TODO: Klima]	[TODO: Brand]	[TODO: Zutritt]

### 69.10.3 Kritische Infrastruktur

Asset-ID	Name	Typ	Standort	Kapazität	Redundanz	Owner	Kritikalität
INFRA-001	USV Anlage 1	USV	SITE-001	[TODO: kVA]	N+1	Facility Management	Tier 1
INFRA-002	Klimaanlage 1	Klimatisator	SITE-001	[TODO: kW]	N+1	Facility Management	Tier 1
INFRA-003	NotstromGenerator	Generator	SITE-001	[TODO: kW]	N	Facility Management	Tier 1
[TODO]	[TODO: Name]	[TODO: Typ]	[TODO: Standort]	[TODO: Kapazität]	[TODO: Redundanz]	[TODO: Owner]	[TODO: [TODO: Tier]]

## 69.11 Asset Lifecycle Management

### 69.11.1 Lifecycle-Phasen

Phase	Beschreibung	Verantwortlich	Prozess
<b>Planung</b>	Bedarfsermittlung, Budgetierung	Business Owner	Anforderungsmanagement
<b>Beschaffung</b>	Auswahl, Bestellung, Lieferung	Procurement	Beschaffungsprozess
<b>Inbetriebnahme</b>	Installation, Konfiguration, Tests	IT Operations	Change Management
<b>Betrieb</b>	Nutzung, Wartung, Monitoring	IT Operations	Betriebsprozesse
<b>Wartung</b>	Updates, Patches, Reparaturen	IT Operations	Patch Management
<b>Außenbetrieb</b>	Dekommissionierung, Datenlöschung	IT Operations	Decommissioning Process
<b>Entsorgung</b>	Sichere Entsorgung oder Wiederverwendung	IT Operations	Disposal Process

### 69.11.2 Asset Owner und Verantwortlichkeiten

Rolle	Verantwortlichkeiten	Kontakt
<b>Asset Owner</b>	Geschäftliche Verantwortung, Genehmigungen, Budget	[TODO: Name/Abteilung]

Rolle	Verantwortlichkeiten	Kontakt
<b>Technical Owner</b>	Technische Verantwortung, Betrieb, Wartung	IT Operations
<b>Security Owner</b>	Sicherheitsanforderungen, Risikobewertung	Thomas Weber
<b>Data Owner</b>	Datenklassifizierung, Zugriffskontrolle	[TODO: Name/Abteilung]

## 69.12 Asset-Tagging und Kennzeichnung

### 69.12.1 Tagging-Schema

Alle Assets werden mit folgenden Tags versehen:

Tag-Kategorie	Beschreibung	Beispiel
<b>Environment</b>	Umgebung	Production, Development, Test, QA
<b>Criticality</b>	Kritikalität	Tier1, Tier2, Tier3, Tier4
<b>Owner</b>	Verantwortlicher	IT-Ops, Security, Development
<b>CostCenter</b>	Kostenstelle	[TODO: Kostenstellen]
<b>Project</b>	Projekt	[TODO: Projektname]
<b>Compliance</b>	Compliance-Anforderungen	PCI-DSS, GDPR, ISO27001

**Hinweis:** Tagging wird in CMDB/Asset Management System gepflegt.

## 69.13 Inventarisierungsprozess

### 69.13.1 Regelmäßige Überprüfung

Aktivität	Frequenz	Verantwortlich	Dokumentation
<b>Vollständige Inventur</b>	Jährlich	Asset Management Team	Inventurbericht
<b>Quartalsweise Überprüfung</b>	Quartalsweise	Asset Owners	Review-Protokoll
<b>Automatische Discovery</b>	Täglich	IT Operations	Discovery Logs
<b>Änderungsverfolgung</b>	Kontinuierlich	Change Management	Change Records

### 69.13.2 Discovery-Tools

Tool	Zweck	Abdeckung	Owner
NetBox	Netzwerk- und Infrastruktur-Inventar	Netzwerkgeräte, Server, VLANs	Network Team
CMDB	Configuration Management Database	Alle IT-Assets	IT Operations
MDM	Mobile Device Management	Endpoints, Mobile Devices	IT Operations
Cloud Asset Inventory	Cloud Resources	Cloud Services	Cloud Team
[TODO: Tool]	[TODO: Zweck]	[TODO: Abdeckung]	[TODO: Owner]

## 69.14 Compliance und Audit

### 69.14.1 Audit-Anforderungen

Dieses Inventar erfüllt folgende Compliance-Anforderungen:

- ISO/IEC 27001:2022 Annex A 5.9: Inventory of Information and Other Associated Assets
- ISO/IEC 27001:2022 Annex A 5.10: Acceptable Use of Information and Other Associated Assets
- ISO/IEC 27001:2022 Annex A 8.9: Configuration Management
- [TODO: Weitere Compliance-Anforderungen]

### 69.14.2 Audit Trail

Datum	Änderung	Durchgeführt von	Genehmigt von	Grund
{} meta.document.erstellung {}}	Initiale Erstellung	{} meta.document.author	Thomas Weber	ISMS-Implementierung
[TODO: Datum]	[TODO: Änderung]	[TODO: Name]	[TODO: Name]	[TODO: Grund]

## 69.15 Referenzen

- Policy: 0300\_Policy\_Asset\_Management.md
- Richtlinie: 0310\_Richtlinie\_Asset\_Inventory\_Tagging\_und\_Entsorgung.md
- Dokument: 0100\_ISMS\_Statement\_of\_Applicability\_SoA\_Template.md
- Anhang: 0730\_Anhang\_Datenfluss\_und\_Schnittstellen\_Template.md

**Dokumentverantwortlicher:** Asset Management Team

**Genehmigt durch:** Thomas Weber

**Nächste Überprüfung:** Quartalsweise

ewpage

# Chapter 70

## Anhang C: Datenfluss und Schnittstellen

**Dokumenttyp:** Anhang

**Version:** 1.0.0

**Datum:** {{ meta.document.date }}

**Klassifizierung:** internal

---

### 70.1 Zweck

Dieses Dokument dokumentiert alle Datenflüsse und Schnittstellen innerhalb der Organisation sowie zu externen Partnern und Dienstleistern. Es erfüllt die Anforderungen von:

- ISO/IEC 27001:2022 Annex A 5.14 (Information Transfer)
- ISO/IEC 27001:2022 Annex A 5.19-5.23 (Supplier Relationships)
- ISO/IEC 27001:2022 Annex A 8.20-8.22 (Network Security)

Die Dokumentation dient als Grundlage für:

- Risikobewertung von Datenübertragungen
- Sicherheitsanforderungen für Schnittstellen
- Datenschutz-Folgenabschätzungen (DPIA)
- Incident Response und Forensik

### 70.2 Geltungsbereich

**Organisation:** AdminSend GmbH

**ISMS Scope:** {{ meta.isms.scope }}

**Verantwortlich:** Thomas Weber, Data Protection Officer

---

## 70.3 Datenfluss-Kategorien

### 70.3.1 Interne Datenflüsse

Datenübertragungen innerhalb der Organisation zwischen verschiedenen Systemen und Standorten.

### 70.3.2 Externe Datenflüsse

Datenübertragungen zwischen der Organisation und externen Partnern, Kunden, Lieferanten oder Cloud-Diensten.

### 70.3.3 Grenzüberschreitende Datenflüsse

Datenübertragungen über Ländergrenzen hinweg, die besondere Datenschutzanforderungen (DS-GVO Art. 44-50) erfüllen müssen.

---

## 70.4 Datenklassifizierung

Alle Datenflüsse werden nach folgenden Klassifizierungen bewertet:

Klassifizierung	Beschreibung	Beispiele	Schutzmaßnahmen
<b>Öffentlich</b>	Für die Öffentlichkeit bestimmt	Marketing-Materialien, öffentliche Website	Keine besonderen Maßnahmen
<b>Intern</b>	Nur für interne Nutzung	Interne Dokumente, Betriebshandbücher	Zugriffskontrolle
<b>Vertraulich</b>	Sensible Geschäftsinformationen	Verträge, Finanzberichte	Verschlüsselung, strenge Zugriffskontrolle
<b>Streng Vertraulich</b>	Höchst sensible Daten	Personenbezogene Daten, Geschäftsgeheimnisse	Ende-zu-Ende-Verschlüsselung, MFA, Audit Logging

---

## 70.5 Interne Datenflüsse

### 70.5.1 Anwendungs-zu-Anwendungs Kommunikation

Datenfluss-							
ID	Quelle	Ziel	Protokoll	Port	Datentyp	Klassifizierung	Verschlüsselung Frequenz
DF-INT-001	[TODO: [TODO: ERP System]	HTTPS CRM System]	443	Kundendaten	Vertraulich	TLS 1.3	Echtzeit
DF-INT-002	[TODO: [TODO: App Server]	PostgreSQL Database]	5432	Transaktionsdaten	Vertraulich	TLS 1.2+	Kontinuierlich
DF-INT-003	[TODO: [TODO: Backup System]	iSCSI Storage]	3260	Backup-Daten	Vertraulich	IPSec	Täglich
[TODO]	[TODO: [TODO: Quelle]	[TODO: Ziel]	[TODO: Protokoll]	[TODO: Port]	[TODO: Datentyp]	[TODO: Klassifizierung]	[TODO: Verschlüsselung]
							[TODO: Frequenz]

**Sicherheitsmaßnahmen:** - Netzwerksegmentierung zwischen Anwendungs- und Datenbankschicht - Firewall-Regeln mit Least-Privilege-Prinzip - Verschlüsselte Verbindungen (TLS 1.2+) - Authentifizierung über Zertifikate oder Service Accounts

### 70.5.2 Site-to-Site Verbindungen

Datenfluss-ID	Quelle-Standort	Ziel-Standort	Verbindungstyp	Bandbreite	Datentyp	Verschlüsselung	Redundanz
DF-S2S-001	{} net-box.site.name {{}}	[TODO: Zweig- stelle]	MPLS	[TODO: Mbps]	Alle Geschäftsdaten	IPSec AES-256	Ja
DF-S2S-002	{} net-box.site.name {{}}	[TODO: DR- Standort]	Dedicated Line	[TODO: Mbps]	Replikation	AES-256	Ja
[TODO]	[TODO: Quelle]	[TODO: Ziel]	[TODO: Typ]	[TODO: Bandbreite]	[TODO: Datentyp]	[TODO: Verschlüsselung]	[TODO: Redundanz]

**Sicherheitsmaßnahmen:** - VPN-Tunnel mit IPSec oder WireGuard - Redundante Verbindungen für kritische Standorte - Monitoring und Alerting bei Verbindungsaußfällen - Regelmäßige Sicherheitsaudits

### 70.5.3 Datenbank-Replikation

Datenfluss-ID	Primäre DB	Sekundäre DB	Replikationstyp	Datentyp	Klassifizierung	Verschlüsselung	RPO
DF-REP-001	[TODO: Prod DB]	[TODO: DR DB]	Asynchron	Alle Produktdaten	Streng Vertraulich	TLS 1.3	< 1h
DF-REP-002	[TODO: Prod DB]	[TODO: Reporting DB]	Synchron	Reporting Daten	Vertraulich	TLS 1.2	< 5min
[TODO]	[TODO: Primär]	[TODO: Sekundär]	[TODO: Typ]	[TODO: Daten- typ]	[TODO: Klassifi- zierung]	[TODO: Ver- schlüsselung]	[TODO: RPO]

## 70.6 Externe Datenflüsse

### 70.6.1 Cloud Services

Datenfluss-ID	Internes System	Cloud Service	Provider	Datentyp	Klassifizierung	Verschlüsselung	Datenstandort
DF-EXT-001	[TODO: File Server]	Microsoft 365	Microsoft	Dokumente, E-Mails	Vertraulich	TLS 1.3, At-Rest AES-256	EU
DF-EXT-002	[TODO: App Server]	AWS S3	Amazon	Backup-Daten	Vertraulich	TLS 1.3, SSE-S3	EU (Frankfurt)
DF-EXT-003	[TODO: Monitoring]	Azure Monitor	Microsoft	Logs, Metriken	Intern	TLS 1.3	EU
[TODO]	[TODO: System]	[TODO: Service]	[TODO: Provider]	[TODO: Daten- typ]	[TODO: Klassifi- zierung]	[TODO: Verschlüs- selung]	[TODO: Standort]

**Sicherheitsmaßnahmen:** - Cloud Security Posture Management (CSPM) - Identity and Access Management (IAM) mit Least Privilege - Verschlüsselung in Transit und At-Rest - Regelmäßige Security Assessments der Cloud Provider - Data Residency Compliance (DSGVO)

### 70.6.2 Partner-Schnittstellen

Datenfluss-ID	Internes System	Partner	Schnittstellentyp	Datentyp	Klassifizierung	Verschlüsselung	Vertrag
DF-PART-001	[TODO: ERP]	Lieferant A]	[TODO: REST API	Bestelldaten	Vertraulich	TLS 1.3, API Key	[TODO: Vertragsnr.]
DF-PART-002	[TODO: CRM]	Part-ner B]	[TODO: SFTP	Kundendaten	Steueng	SSH, PGP	[TODO: Vertragsnr.]
[TODO]	[TODO: System]	Part-ner]	[TODO: [TODO: Typ]	[TODO: Daten- typ]	[TODO: Klassifi- zierung]	[TODO: Verschlüs- selung]	[TODO: Vertrag]

**Sicherheitsmaßnahmen:** - Supplier Security Assessments vor Vertragsabschluss - Data Processing Agreements (DPA) gemäß DSGVO Art. 28 - Mutual TLS (mTLS) für API-Kommunikation - API Rate Limiting und Monitoring - Regelmäßige Sicherheitsaudits

---

### 70.6.3 Kunden-Schnittstellen

Datenfluss-ID	Internes System	Schnittstelle	Protokoll	Datentyp	Klassifizierung	Verschlüsselung	Authentifizierung
DF-CUST-001	[TODO: Web App]	Kundenportal	HTTPS	Kundendaten	Steueng	TLS 1.3	OAuth 2.0 + MFA
DF-CUST-002	[TODO: API Gateway]	Mobile App	HTTPS	Transaktionsdaten	Vertraulich	TLS 1.3	JWT + Biometrie
[TODO]	[TODO: System]	[TODO: Schnittstelle]	[TODO: Protokoll]	[TODO: Daten- typ]	[TODO: Klassifi- zierung]	[TODO: Verschlüs- selung]	[TODO: Auth]

**Sicherheitsmaßnahmen:** - Web Application Firewall (WAF) - DDoS Protection - Rate Limiting und Throttling - Input Validation und Output Encoding - Security Headers (HSTS, CSP, etc.)

---

## 70.7 Grenzüberschreitende Datenflüsse

### 70.7.1 EU-Drittland-Transfers

Datenfluss-ID	Quelle (EU)	Ziel (Drittland)	Land	Datentyp	Rechtsgrundlage	Schutzmaßnahmen
DF-CROSS-001	<pre>{{   net-   box.site.name }}</pre> <p>[TODO]</p>	<p>[TODO: US-Rechenzentrum]</p> <p>[TODO: Ziel] Quelle]</p>	USA	Cloud-Daten	Standard Contractual Clauses (SCC)	Verschlüsselung, Access Controls
			[TODO: Land]	Daten-typ]	[TODO: Rechtsgrund-lage]	[TODO: Maßnahmen]

**DSGVO-Compliance:** - Art. 44-50 DSGVO: Datenübermittlung in Drittländer - Standard Contractual Clauses (SCC) gemäß Art. 46 Abs. 2 lit. c DSGVO - Transfer Impact Assessment (TIA) durchgeführt - Zusätzliche Schutzmaßnahmen implementiert

---

## 70.8 Schnittstellen-Dokumentation

### 70.8.1 API-Schnittstellen

API-ID	Name	Typ	Version	Authentifizierung	Autorisierung	Rate Limit	Dokumentation
API-001	[TODO: REST v2.0 Customer API]			OAuth 2.0	RBAC	1000 req/min	[TODO: URL]
API-002	[TODO: REST v1.5 Partner API]			API Key + mTLS	API Key Scopes	500 req/min	[TODO: URL]
API-003	[TODO: GraphQL Internal API]			JWT	ABAC	Unbegrenzt	[TODO: URL]
[TODO]	[TODO: [TODO: Name] Typ]	[TODO: Version]		[TODO: Auth]	[TODO: Authz]	[TODO: Limit]	[TODO: Docs]

**Sicherheitsanforderungen:** - API Gateway mit Authentifizierung und Autorisierung - Input Validation und Schema Validation - Output Filtering (keine sensiblen Daten in Fehlermeldungen) - Logging und Monitoring aller API-Zugriffe - Versionierung und Deprecation Policy

---

### 70.8.2 Datei-Transfer-Schnittstellen

Schnittstellen-ID	Typ	Protokoll	Quelle	Ziel	Datentyp	Verschlüsselung	Authentifizierung
FT-001	SFTP	SSH	[TODO: System]	[TODO: Partner]	[TODO: Dateien]	SSH, PGP	SSH Key
FT-002	FTPS	FTP over TLS	[TODO: System]	[TODO: System]	[TODO: Dateien]	TLS 1.3	Zertifikat
FT-003	MFT	Managed File Transfer	[TODO: System]	[TODO: Partner]	[TODO: Geschäftsdaten]	AES-256	OAuth 2.0
[TODO]	[TODO: Typ]	[TODO: Protokoll]	[TODO: Quelle]	[TODO: Ziel]	[TODO: Daten- typ]	[TODO: Verschlüsselung]	[TODO: Auth]

### 70.8.3 Messaging-Schnittstellen

Schnittstellen-ID	Typ	Protokoll	Quelle	Ziel	Nachrichtentyp	Verschlüsselung	Persistenz
MSG-001	Message Queue	AMQP	[TODO: Producer]	[TODO: Consumer]	[TODO: Events]	TLS 1.3	7 Tage
MSG-002	Event Stream	Kafka	[TODO: Producer]	[TODO: Consumer]	[TODO: Logs]	TLS 1.3	30 Tage
[TODO]	[TODO: Typ]	[TODO: Protokoll]	[TODO: Quelle]	[TODO: Ziel]	[TODO: Nachrichtentyp]	[TODO: Verschlüsselung]	[TODO: Persistenz]

### 70.8.4 E-Mail-Kommunikation

Kommunikationsart	Absender	Empfänger	Datentyp	Klassifizierung	Verschlüsselung	Archivierung
Geschäfts-E-Mail	{} meta.organization.domain	Extern	Geschäftskontakt	Vertraulich	TLS (Opportunistic)	7 Jahre
Vertrauliche E-Mail	{} meta.organization.domain	Extern	Vertragsdokument	Strategisch	S/MIME oder PGP	10 Jahre
Interne E-Mail	{} meta.organization.domain	{} meta.organization.domain	Interne Organisation	Intern	TLS (Enforced)	3 Jahre

**Sicherheitsmaßnahmen:** - SPF, DKIM, DMARC für E-Mail-Authentifizierung - E-Mail Gateway mit Anti-Spam und Anti-Malware - Data Loss Prevention (DLP) für ausgehende E-Mails - E-Mail-Verschlüsselung für vertrauliche Inhalte - E-Mail-Archivierung gemäß gesetzlichen Anforderungen

---

## 70.9 Netzwerk-Architektur

### 70.9.1 Netzwerk-Zonen

Zone	Beschreibung	Sicherheitsstufe	Zugriffskontrolle	Systeme
<b>DMZ</b>	Demilitarisierte Zone für öffentlich zugängliche Dienste	Hoch	Firewall, IDS/IPS	Web Server, Mail Gateway
<b>Internal</b>	Internes Netzwerk für Geschäftsanwendungen	Mittel	Firewall, NAC	App Server, File Server
<b>Management</b>	Management-Netzwerk für Administration	Sehr Hoch	Firewall, MFA, Jump Host	Management Interfaces
<b>Production</b>	Produktionsnetzwerk für kritische Systeme	Sehr Hoch	Firewall, Segmentierung	Database Server, Core Systems
<b>Development</b>	Entwicklungs- und Testnetzwerk	Niedrig	Firewall	Dev/Test Systems

---

### 70.9.2 Firewall-Regeln (Beispiel)

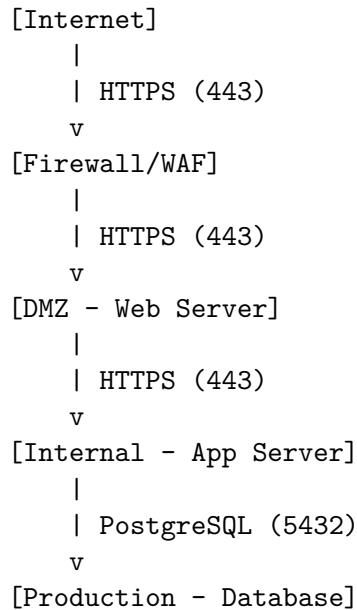
Regel-ID	Quelle-Zone	Ziel-Zone	Protokoll	Port	Aktion	Logging	Beschreibung
FW-001	Internet	DMZ	HTTPS	443	Allow	Ja	Web-Traffic zu Web Servern
FW-002	DMZ	Internal	HTTPS	443	Allow	Ja	Web Server zu App Server
FW-003	Internal	Production	PostgreSQL	5432	Allow	Ja	App Server zu Database
FW-004	Management	All	SSH	22	Allow	Ja	Admin-Zugriff
FW-999	Any	Any	Any	Any	Deny	Ja	Default Deny

**Hinweis:** Vollständige Firewall-Regeln in separater Dokumentation.

---

## 70.10 Datenfluss-Diagramme

### 70.10.1 High-Level Architektur



**Hinweis:** Detaillierte Netzwerkdiagramme in separaten Dateien (z.B. Visio, Draw.io).

---

### 70.10.2 Datenfluss für kritische Geschäftsprozesse

#### 70.10.2.1 Beispiel: Kundenbestellung

[Kunde]

- > HTTPS -> [Web Portal (DMZ)]
- > HTTPS -> [Order Service (Internal)]
- > PostgreSQL -> [Order DB (Production)]
- > HTTPS -> [Payment Gateway (External)]
- > HTTPS -> [ERP System (Internal)]
- > HTTPS -> [Warehouse System (Internal)]

**Sicherheitsmaßnahmen:** - Ende-zu-Ende-Verschlüsselung - Authentifizierung auf jeder Ebene - Input Validation - Audit Logging aller Transaktionen

---

## 70.11 Risikobewertung Datenflüsse

### 70.11.1 Risikomatrix

Datenfluss-ID	Bedrohung	Wahrscheinlichkeit	Auswirkung	Risiko	Maßnahmen	Restrisiko
DF-EXT-001	Datenverlust bei Cloud-Transfer	Niedrig	Hoch	Mittel	Verschlüsselung, DLP	Niedrig
DF-PART-001	Unbefugter Zugriff durch Partner	Mittel	Hoch	Hoch	mTLS, API Gateway, Monitoring	Mittel
DF-CROSS-001	Drittland-Zugriff auf EU-Daten	Mittel	Sehr Hoch	Hoch	SCC, Verschlüsselung, Access Controls	Mittel
[TODO]	[TODO: Bedrohung]	[TODO: W'keit]	[TODO: Auswirkung]	[TODO: Risiko]	[TODO: Maßnahmen]	[TODO: Restrisiko]

## 70.12 Monitoring und Logging

### 70.12.1 Datenfluss-Monitoring

Monitoring-Typ	Tool	Metriken	Alerting	Retention
Network Traffic	[TODO: Net-Flow/sFlow]	Bandbreite, Verbindungen, Anomalien	Ja	90 Tage
API Traffic	[TODO: API Gateway]	Request Rate, Latency, Errors	Ja	90 Tage
Firewall Logs	[TODO: SIEM]	Blocked Connections, Rule Hits	Ja	1 Jahr
Application Logs	[TODO: Log Management]	Transactions, Errors, Security Events	Ja	1 Jahr

### 70.12.2 Security Events

Folgende Security Events werden für Datenflüsse überwacht:

- Ungewöhnliche Datenübertragungsvolumen
- Verbindungen zu unbekannten Zielen
- Fehlgeschlagene Authentifizierungsversuche

- Protokollverletzungen
  - Verschlüsselungsfehler
  - DLP-Verstöße
- 

## 70.13 Compliance und Datenschutz

### 70.13.1 DSGVO-Anforderungen

Anforderung	Artikel	Umsetzung	Nachweis
Rechtmäßigkeit der Verarbeitung	Art. 6	Rechtsgrundlage dokumentiert	Verarbeitungsverzeichnis
Datenminimierung	Art. 5 Abs. 1 lit. c	Nur notwendige Daten übertragen	Datenfluss-Dokumentation
Integrität und Vertraulichkeit	Art. 5 Abs. 1 lit. f	Verschlüsselung, Zugriffskontrolle	Sicherheitsmaßnahmen
Drittland-Transfer	Art. 44-50	SCC, TIA	Transfer-Dokumentation

---

### 70.13.2 Verarbeitungsverzeichnis-Referenz

Alle Datenflüsse sind im Verarbeitungsverzeichnis gemäß Art. 30 DSGVO dokumentiert.

**Referenz:** [TODO: Link zum Verarbeitungsverzeichnis]

---

## 70.14 Änderungsmanagement

### 70.14.1 Change Control

Alle Änderungen an Datenflüssen und Schnittstellen unterliegen dem Change Management Prozess:

1. **Change Request:** Antrag mit Begründung und Risikobewertung
2. **Security Review:** Bewertung durch Security Team
3. **Approval:** Genehmigung durch Change Advisory Board
4. **Implementation:** Umsetzung mit Dokumentation
5. **Verification:** Test und Validierung
6. **Documentation Update:** Aktualisierung dieses Dokuments

**Referenz:** 0360\_Policy\_Change\_und\_Release\_Management.md

---

## 70.15 Referenzen

- Policy: 0660\_Policy\_Informationsübertragung\_und\_Kommunikation.md

- Richtlinie: 0670\_Richtlinie\_Email\_Sharing\_und\_Zusammenarbeitstools.md
  - Policy: 0460\_Policy\_Lieferanten\_und\_Cloud\_Sicherheit.md
  - Richtlinie: 0470\_Richtlinie\_Third\_Party\_Risk\_Assessment\_und\_Cloud\_Controls.md
  - Policy: 0600\_Policy\_Netzwerksicherheit.md
  - Richtlinie: 0610\_Richtlinie\_Segmentierung\_Firewalling\_und\_Network\_Access\_Control.md
  - Anhang: 0720\_Anhang\_Asset\_und\_Systeminventar\_Template.md
- 

**Dokumentverantwortlicher:** Thomas Weber

**Genehmigt durch:** {{ meta.management.name }}

**Nächste Überprüfung:** Halbjährlich

ewpage

# Chapter 71

## Anhang D: Begriffe und Abkürzungen

**Dokumenttyp:** Anhang

**Version:** 1.0.0

**Datum:** {{ meta.document.date }}

**Klassifizierung:** internal

---

### 71.1 Zweck

Dieses Dokument definiert alle im ISMS verwendeten Begriffe und Abkürzungen. Es dient als zentrale Referenz für einheitliche Terminologie und erleichtert das Verständnis der ISMS-Dokumentation.

### 71.2 Geltungsbereich

**Organisation:** AdminSend GmbH

**ISMS Scope:** {{ meta.isms.scope }}

**Verantwortlich:** Thomas Weber

---

### 71.3 Abkürzungen

#### 71.3.1 A

Abkürzung	Bedeutung	Erläuterung
<b>ABAC</b>	Attribute-Based Access Control	Attributbasierte Zugriffskontrolle
<b>ACL</b>	Access Control List	Zugriffskontrollliste
<b>AES</b>	Advanced Encryption Standard	Symmetrischer Verschlüsselungsstandard
<b>API</b>	Application Programming Interface	Programmierschnittstelle

Abkürzung	Bedeutung	Erläuterung
<b>APT</b>	Advanced Persistent Threat	Fortgeschrittene, anhaltende Bedrohung
<b>AV</b>	Antivirus	Antivirenssoftware

### 71.3.2 B

Abkürzung	Bedeutung	Erläuterung
<b>BC</b>	Business Continuity	Geschäftskontinuität
<b>BCP</b>	Business Continuity Plan	Geschäftskontinuitätsplan
<b>BIA</b>	Business Impact Analysis	Geschäftsauwirkungsanalyse
<b>BYOD</b>	Bring Your Own Device	Nutzung privater Geräte für geschäftliche Zwecke

### 71.3.3 C

Abkürzung	Bedeutung	Erläuterung
<b>CA</b>	Certificate Authority	Zertifizierungsstelle
<b>CAB</b>	Change Advisory Board	Änderungsgremium
<b>CIA</b>	Confidentiality, Integrity, Availability	Vertraulichkeit, Integrität, Verfügbarkeit
<b>CISO</b>	Chief Information Security Officer	Informationssicherheitsbeauftragter
<b>CIS</b>	Center for Internet Security	Organisation für Internet-Sicherheitsstandards
<b>CMDB</b>	Configuration Management Database	Konfigurationsdatenbank
<b>CRM</b>	Customer Relationship Management	Kundenbeziehungsmanagement
<b>CSP</b>	Content Security Policy	Inhaltssicherheitsrichtlinie
<b>CSPM</b>	Cloud Security Posture Management	Cloud-Sicherheitslage-Management
<b>CVE</b>	Common Vulnerabilities and Exposures	Gemeinsame Schwachstellen und Expositionen
<b>CVSS</b>	Common Vulnerability Scoring System	Bewertungssystem für Schwachstellen

### 71.3.4 D

Abkürzung	Bedeutung	Erläuterung
<b>DAST</b>	Dynamic Application Security Testing	Dynamische Anwendungssicherheitstests
<b>DDoS</b>	Distributed Denial of Service	Verteilter Denial-of-Service-Angriff

Abkürzung	Bedeutung	Erläuterung
<b>DLP</b>	Data Loss Prevention	Datenverlustprävention
<b>DMZ</b>	Demilitarized Zone	Demilitarisierte Zone
<b>DNS</b>	Domain Name System	Domänennamensystem
<b>DoS</b>	Denial of Service	Dienstverweigerungsangriff
<b>DPA</b>	Data Processing Agreement	Datenverarbeitungsvereinbarung
<b>DPIA</b>	Data Protection Impact Assessment	Datenschutz-Folgenabschätzung
<b>DPO</b>	Data Protection Officer	Datenschutzbeauftragter
<b>DR</b>	Disaster Recovery	Notfallwiederherstellung
<b>DRP</b>	Disaster Recovery Plan	Notfallwiederherstellungsplan
<b>DSGVO</b>	Datenschutz-Grundverordnung	EU-Datenschutzverordnung (GDPR)

#### 71.3.5 E

Abkürzung	Bedeutung	Erläuterung
<b>EDR</b>	Endpoint Detection and Response	Endpunkt-Erkennung und -Reaktion
<b>ERP</b>	Enterprise Resource Planning	Unternehmensressourcenplanung

#### 71.3.6 F

Abkürzung	Bedeutung	Erläuterung
<b>FQDN</b>	Fully Qualified Domain Name	Vollständig qualifizierter Domänenname
<b>FTP</b>	File Transfer Protocol	Dateiübertragungsprotokoll
<b>FTPS</b>	FTP Secure	Sicheres FTP über TLS

#### 71.3.7 G

Abkürzung	Bedeutung	Erläuterung
<b>GDPR</b>	General Data Protection Regulation	Datenschutz-Grundverordnung (DSGVO)

#### 71.3.8 H

Abkürzung	Bedeutung	Erläuterung
<b>HIDS</b>	Host-based Intrusion Detection System	Host-basiertes Intrusion Detection System

Abkürzung	Bedeutung	Erläuterung
<b>HIPS</b>	Host-based Intrusion Prevention System	Host-basiertes Intrusion Prevention System
<b>HSTS</b>	HTTP Strict Transport Security	HTTP Strict Transport Security
<b>HTTP</b>	Hypertext Transfer Protocol	Hypertext-Übertragungsprotokoll
<b>HTTPS</b>	HTTP Secure	Sicheres HTTP über TLS

### 71.3.9 I

Abkürzung	Bedeutung	Erläuterung
<b>IaaS</b>	Infrastructure as a Service	Infrastruktur als Service
<b>IAM</b>	Identity and Access Management	Identitäts- und Zugriffsverwaltung
<b>ICMP</b>	Internet Control Message Protocol	Internet Control Message Protocol
<b>ICT</b>	Information and Communication Technology	Informations- und Kommunikationstechnologie
<b>IDS</b>	Intrusion Detection System	Intrusion Detection System
<b>IG</b>	Implementation Group	Implementierungsgruppe (CIS Controls)
<b>IoC</b>	Indicator of Compromise	Kompromittierungsindikator
<b>IP</b>	Internet Protocol	Internetprotokoll
<b>IPS</b>	Intrusion Prevention System	Intrusion Prevention System
<b>IPSec</b>	Internet Protocol Security	Internet Protocol Security
<b>ISMS</b>	Information Security Management System	Informationssicherheits-Managementsystem
<b>ISO</b>	International Organization for Standardization	Internationale Organisation für Normung
<b>ISP</b>	Internet Service Provider	Internetdienstanbieter
<b>IT</b>	Information Technology	Informationstechnologie

### 71.3.10 J

Abkürzung	Bedeutung	Erläuterung
<b>JWT</b>	JSON Web Token	JSON Web Token

### 71.3.11 K

Abkürzung	Bedeutung	Erläuterung
<b>KPI</b>	Key Performance Indicator	Leistungskennzahl

### 71.3.12 L

Abkürzung	Bedeutung	Erläuterung
<b>LDAP</b>	Lightweight Directory Access Protocol	Lightweight Directory Access Protocol

### 71.3.13 M

Abkürzung	Bedeutung	Erläuterung
<b>MAC</b>	Media Access Control / Mandatory Access Control	MAC-Adresse / Obligatorische Zugriffskontrolle
<b>MDM</b>	Mobile Device Management	Mobile Geräteverwaltung
<b>MFA</b>	Multi-Factor Authentication	Mehr-Faktor-Authentifizierung
<b>MFT</b>	Managed File Transfer	Verwaltete Dateiübertragung
<b>MPLS</b>	Multiprotocol Label Switching	Multiprotocol Label Switching
<b>mTLS</b>	Mutual TLS	Gegenseitiges TLS

### 71.3.14 N

Abkürzung	Bedeutung	Erläuterung
<b>NAC</b>	Network Access Control	Netzwerkzugriffskontrolle
<b>NDA</b>	Non-Disclosure Agreement	Geheimhaltungsvereinbarung
<b>NIDS</b>	Network-based Intrusion Detection System	Netzwerkbasiertes Intrusion Detection System
<b>NIPS</b>	Network-based Intrusion Prevention System	Netzwerkbasiertes Intrusion Prevention System
<b>NTP</b>	Network Time Protocol	Netzwerkzeitprotokoll

### 71.3.15 O

Abkürzung	Bedeutung	Erläuterung
<b>OAuth</b>	Open Authorization	Offenes Autorisierungsprotokoll
<b>OWASP</b>	Open Web Application Security Project	Open Web Application Security Project

### 71.3.16 P

Abkürzung	Bedeutung	Erläuterung
<b>PaaS</b>	Platform as a Service	Plattform als Service
<b>PAM</b>	Privileged Access Management	Privilegierte Zugriffsverwaltung

Abkürzung	Bedeutung	Erläuterung
<b>PCI DSS</b>	Payment Card Industry Data Security Standard	Zahlungskartenindustrie-Datensicherheitsstandard
<b>PGP</b>	Pretty Good Privacy	Pretty Good Privacy (Verschlüsselung)
<b>PII</b>	Personally Identifiable Information	Personenbezogene Daten
<b>PKI</b>	Public Key Infrastructure	Public-Key-Infrastruktur

### 71.3.17 R

Abkürzung	Bedeutung	Erläuterung
<b>RACI</b>	Responsible, Accountable, Consulted, Informed	Verantwortlichkeitsmatrix
<b>RBAC</b>	Role-Based Access Control	Rollenbasierte Zugriffskontrolle
<b>REST</b>	Representational State Transfer	Representational State Transfer
<b>RPO</b>	Recovery Point Objective	Wiederherstellungspunktziel
<b>RTO</b>	Recovery Time Objective	Wiederherstellungszeitziel

### 71.3.18 S

Abkürzung	Bedeutung	Erläuterung
<b>SaaS</b>	Software as a Service	Software als Service
<b>SAML</b>	Security Assertion Markup Language	Security Assertion Markup Language
<b>SAN</b>	Storage Area Network	Speichernetzwerk
<b>SAST</b>	Static Application Security Testing	Statische Anwendungssicherheitstests
<b>SCC</b>	Standard Contractual Clauses	Standardvertragsklauseln
<b>SDLC</b>	Software Development Life Cycle	Software-Entwicklungslebenszyklus
<b>SFTP</b>	SSH File Transfer Protocol	SSH File Transfer Protocol
<b>SIEM</b>	Security Information and Event Management	Sicherheitsinformations- und Ereignisverwaltung
<b>SLA</b>	Service Level Agreement	Dienstgütevereinbarung
<b>S/MIME</b>	Secure/Multipurpose Internet Mail Extensions	Sichere E-Mail-Verschlüsselung
<b>SMB</b>	Server Message Block	Server Message Block
<b>SMTP</b>	Simple Mail Transfer Protocol	Simple Mail Transfer Protocol
<b>SoA</b>	Statement of Applicability	Anwendbarkeitserklärung
<b>SOAP</b>	Simple Object Access Protocol	Simple Object Access Protocol

Abkürzung	Bedeutung	Erläuterung
<b>SOC</b>	Security Operations Center	Sicherheitsbetriebszentrum
<b>SOP</b>	Standard Operating Procedure	Standardbetriebsverfahren
<b>SPF</b>	Sender Policy Framework	Sender Policy Framework
<b>SQL</b>	Structured Query Language	Structured Query Language
<b>SSH</b>	Secure Shell	Secure Shell
<b>SSL</b>	Secure Sockets Layer	Secure Sockets Layer (veraltet, siehe TLS)
<b>SSO</b>	Single Sign-On	Einmalige Anmeldung

### 71.3.19 T

Abkürzung	Bedeutung	Erläuterung
<b>TCP</b>	Transmission Control Protocol	Transmission Control Protocol
<b>TIA</b>	Transfer Impact Assessment	Transfer-Folgenabschätzung
<b>TLS</b>	Transport Layer Security	Transport Layer Security
<b>TPP</b>	Tactics, Techniques, and Procedures	Taktiken, Techniken und Verfahren

### 71.3.20 U

Abkürzung	Bedeutung	Erläuterung
<b>UDP</b>	User Datagram Protocol	User Datagram Protocol
<b>URL</b>	Uniform Resource Locator	Uniform Resource Locator
<b>USV</b>	Unterbrechungsfreie Stromversorgung	Unterbrechungsfreie Stromversorgung (UPS)

### 71.3.21 V

Abkürzung	Bedeutung	Erläuterung
<b>VLAN</b>	Virtual Local Area Network	Virtuelles lokales Netzwerk
<b>VPN</b>	Virtual Private Network	Virtuelles privates Netzwerk

### 71.3.22 W

Abkürzung	Bedeutung	Erläuterung
<b>WAF</b>	Web Application Firewall	Web Application Firewall
<b>WAN</b>	Wide Area Network	Weitverkehrsnetz

### 71.3.23 X

Abkürzung	Bedeutung	Erläuterung
XSS	Cross-Site Scripting	Cross-Site Scripting

### 71.3.24 Z

Abkürzung	Bedeutung	Erläuterung
ZTA	Zero Trust Architecture	Zero-Trust-Architektur

## 71.4 Begriffsdefinitionen

### 71.4.1 A

#### **Acceptable Use Policy (AUP)**

Richtlinie, die die akzeptable Nutzung von IT-Ressourcen definiert.

#### **Access Control**

Zugriffskontrolle; Mechanismen zur Steuerung des Zugriffs auf Ressourcen.

#### **Accountability**

Rechenschaftspflicht; die Verantwortung für Handlungen und Entscheidungen.

#### **Advanced Persistent Threat (APT)**

Fortgeschrittene, anhaltende Bedrohung; gezielte, langfristige Cyberangriffe.

#### **Annex A**

Anhang A der ISO/IEC 27001, der 93 Sicherheitskontrollen definiert.

#### **Asset**

Vermögenswert; jede Ressource mit Wert für die Organisation (Hardware, Software, Daten, etc.).

#### **Audit**

Systematische, unabhängige Überprüfung zur Feststellung der Konformität.

#### **Authentication**

Authentifizierung; Nachweis der Identität eines Benutzers oder Systems.

#### **Authorization**

Autorisierung; Gewährung von Zugriffsrechten nach erfolgreicher Authentifizierung.

#### **Availability**

Verfügbarkeit; Eigenschaft, dass Informationen und Systeme bei Bedarf zugänglich sind.

## **71.4.2 B**

### **Backup**

Sicherungskopie von Daten zur Wiederherstellung im Fehlerfall.

### **Baseline**

Ausgangsbasis; definierter Zustand als Referenz für Änderungen.

### **Business Continuity**

Geschäftskontinuität; Fähigkeit, Geschäftsprozesse bei Störungen aufrechtzuerhalten.

### **Business Impact Analysis (BIA)**

Geschäftsauswirkungsanalyse; Bewertung der Auswirkungen von Störungen auf Geschäftsprozesse.

---

## **71.4.3 C**

### **Change Management**

Änderungsmanagement; kontrollierter Prozess zur Durchführung von Änderungen.

### **CIA Triad**

CIA-Triade; Grundprinzipien der Informationssicherheit (Confidentiality, Integrity, Availability).

### **Cloud Computing**

Bereitstellung von IT-Ressourcen über das Internet.

### **Compliance**

Einhaltung von Gesetzen, Vorschriften und Standards.

### **Confidentiality**

Vertraulichkeit; Schutz von Informationen vor unbefugter Offenlegung.

### **Configuration Management**

Konfigurationsmanagement; Verwaltung und Kontrolle von Systemkonfigurationen.

### **Control**

Kontrolle/Maßnahme; Sicherheitsmaßnahme zur Risikominderung.

### **Cryptography**

Kryptografie; Wissenschaft der Verschlüsselung und Entschlüsselung von Informationen.

### **Cyber Security**

Cybersicherheit; Schutz von Computersystemen und Netzwerken vor Angriffen.

---

## **71.4.4 D**

### **Data Breach**

Datenpanne; unbefugter Zugriff auf oder Offenlegung von Daten.

### **Data Classification**

Datenklassifizierung; Kategorisierung von Daten nach Schutzbedarf.

**Data Loss Prevention (DLP)**

Datenverlustprävention; Technologien zum Schutz vor Datenverlust.

**Data Protection**

Datenschutz; Schutz personenbezogener Daten.

**Disaster Recovery**

Notfallwiederherstellung; Wiederherstellung von IT-Systemen nach einem Ausfall.

---

**71.4.5 E****Encryption**

Verschlüsselung; Umwandlung von Daten in unlesbares Format.

**Endpoint**

Endgerät; Gerät am Ende einer Netzwerkverbindung (PC, Laptop, Smartphone).

**Event**

Ereignis; identifizierbare Zustandsänderung in einem System.

---

**71.4.6 F****Firewall**

Firewall; Sicherheitssystem zur Kontrolle des Netzwerkverkehrs.

**Forensics**

Forensik; Untersuchung von Sicherheitsvorfällen.

---

**71.4.7 G****Gap Analysis**

Lückenanalyse; Vergleich zwischen Ist- und Soll-Zustand.

**Governance**

Governance; Rahmenwerk für Führung und Kontrolle.

---

**71.4.8 H****Hardening**

Härtung; Absicherung von Systemen durch Entfernung unnötiger Funktionen.

**Hash**

Hash; eindeutige Prüfsumme zur Integritätssicherung.

---

## **71.4.9 I**

### **Incident**

Vorfall; Ereignis, das die Informationssicherheit beeinträchtigt.

### **Incident Response**

Vorfallreaktion; Prozess zur Behandlung von Sicherheitsvorfällen.

### **Information Security**

Informationssicherheit; Schutz von Informationen vor Bedrohungen.

### **Integrity**

Integrität; Eigenschaft, dass Informationen vollständig und unverändert sind.

### **Intrusion Detection**

Einbruchserkennung; Erkennung von Angriffen auf Systeme.

---

## **71.4.10 K**

### **Key Management**

Schlüsselverwaltung; Verwaltung kryptografischer Schlüssel.

---

## **71.4.11 L**

### **Least Privilege**

Minimale Rechtevergabe; Prinzip, nur notwendige Zugriffsrechte zu gewähren.

### **Logging**

Protokollierung; Aufzeichnung von Ereignissen und Aktivitäten.

---

## **71.4.12 M**

### **Malware**

Schadsoftware; Software mit schädlicher Absicht.

### **Management Review**

Managementbewertung; regelmäßige Überprüfung des ISMS durch das Management.

### **Monitoring**

Überwachung; kontinuierliche Beobachtung von Systemen und Prozessen.

### **Multi-Factor Authentication (MFA)**

Mehr-Faktor-Authentifizierung; Authentifizierung mit mehreren Faktoren.

---

## **71.4.13 N**

### **Network Segmentation**

Netzwerksegmentierung; Aufteilung eines Netzwerks in separate Bereiche.

## **Non-Conformity**

Nichtkonformität; Abweichung von Anforderungen.

---

### **71.4.14 P**

#### **Patch Management**

Patch-Management; Prozess zur Verwaltung von Software-Updates.

#### **Penetration Testing**

Penetrationstest; simulierter Angriff zur Identifikation von Schwachstellen.

#### **Phishing**

Phishing; Versuch, durch gefälschte Nachrichten an sensible Daten zu gelangen.

#### **Policy**

Richtlinie; formale Regel oder Grundsatz der Organisation.

#### **Privacy**

Privatsphäre; Recht auf Schutz personenbezogener Daten.

#### **Privileged Access**

Privilegierter Zugriff; Zugriff mit erweiterten Rechten.

---

### **71.4.15 R**

#### **Ransomware**

Ransomware; Schadsoftware, die Daten verschlüsselt und Lösegeld fordert.

#### **Recovery Point Objective (RPO)**

Wiederherstellungspunktziel; maximal akzeptabler Datenverlust.

#### **Recovery Time Objective (RTO)**

Wiederherstellungszeitziel; maximal akzeptable Ausfallzeit.

#### **Residual Risk**

Restrisiko; verbleibendes Risiko nach Implementierung von Maßnahmen.

#### **Risk**

Risiko; Kombination aus Eintrittswahrscheinlichkeit und Auswirkung einer Bedrohung.

#### **Risk Assessment**

Risikobewertung; Prozess zur Identifikation und Bewertung von Risiken.

#### **Risk Treatment**

Risikobehandlung; Maßnahmen zur Risikominderung.

---

### **71.4.16 S**

#### **Security Awareness**

Sicherheitsbewusstsein; Wissen und Verständnis für Informationssicherheit.

**Security Control**

Sicherheitskontrolle; Maßnahme zur Risikominderung.

**Security Incident**

Sicherheitsvorfall; Ereignis, das die Informationssicherheit beeinträchtigt.

**Security Policy**

Sicherheitsrichtlinie; formale Regel zur Informationssicherheit.

**Segregation of Duties**

Funktionstrennung; Aufteilung von Aufgaben zur Vermeidung von Interessenkonflikten.

**Social Engineering**

Social Engineering; Manipulation von Personen zur Preisgabe von Informationen.

**Statement of Applicability (SoA)**

Anwendbarkeitserklärung; Dokument, das die Anwendbarkeit von Kontrollen erklärt.

**Supply Chain**

Lieferkette; Netzwerk von Lieferanten und Dienstleistern.

---

**71.4.17 T****Threat**

Bedrohung; potenzielle Ursache eines unerwünschten Ereignisses.

**Threat Intelligence**

Bedrohungsinformationen; Informationen über aktuelle Bedrohungen.

**Two-Factor Authentication (2FA)**

Zwei-Faktor-Authentifizierung; Authentifizierung mit zwei Faktoren.

---

**71.4.18 V****Vulnerability**

Schwachstelle; Schwäche, die von einer Bedrohung ausgenutzt werden kann.

**Vulnerability Assessment**

Schwachstellenbewertung; Identifikation und Bewertung von Schwachstellen.

---

**71.4.19 W****Whitelist**

Whitelist; Liste erlaubter Elemente (Anwendungen, IP-Adressen, etc.).

---

## 71.4.20 Z

### **Zero Day**

Zero-Day; Schwachstelle, für die noch kein Patch verfügbar ist.

### **Zero Trust**

Zero Trust; Sicherheitsmodell ohne implizites Vertrauen.

---

## 71.5 ISO/IEC 27001:2022 Spezifische Begriffe

### **Annex A Control**

Eine der 93 Sicherheitskontrollen aus Annex A der ISO/IEC 27001:2022.

### **Context of the Organization**

Kontext der Organisation; Verständnis interner und externer Faktoren (Klausel 4).

### **Continual Improvement**

Kontinuierliche Verbesserung; fortlaufende Verbesserung des ISMS (Klausel 10).

### **Documented Information**

Dokumentierte Information; Informationen, die dokumentiert und aufbewahrt werden müssen.

### **Interested Party**

Interessierte Partei; Person oder Organisation, die das ISMS beeinflussen kann.

### **Internal Audit**

Internes Audit; systematische Überprüfung des ISMS (Klausel 9.2).

### **ISMS Scope**

ISMS-Geltungsbereich; Grenzen und Anwendbarkeit des ISMS (Klausel 4.3).

### **Leadership**

Führung; Verpflichtung und Engagement des Top-Managements (Klausel 5).

### **Management Review**

Managementbewertung; regelmäßige Überprüfung durch das Management (Klausel 9.3).

### **Performance Evaluation**

Leistungsbewertung; Überwachung, Messung und Bewertung des ISMS (Klausel 9).

### **Risk Assessment**

Risikobewertung; Prozess zur Identifikation und Bewertung von Risiken (Klausel 6.1.2).

### **Risk Treatment**

Risikobehandlung; Auswahl und Implementierung von Maßnahmen (Klausel 6.1.3).

### **Statement of Applicability (SoA)**

Anwendbarkeitserklärung; Dokument mit Annex A Kontrollen und deren Anwendbarkeit (Klausel 6.1.3).

---

## 71.6 Referenzen

- ISO/IEC 27000:2018 Information Security Management Systems - Overview and Vocabulary
  - ISO/IEC 27001:2022 Information Security Management Systems - Requirements
  - ISO/IEC 27002:2022 Information Security Controls
  - NIST Glossary: <https://csrc.nist.gov/glossary>
- 

**Dokumentverantwortlicher:** Thomas Weber

**Genehmigt durch:** {{ meta.management.name }}

**Nächste Überprüfung:** Jährlich

ewpage