



Informationssicherheits- managementsystem für kleine und mittlere Unternehmen (KMU)

Anforderungen

Herausgeber und Verlag: VdS Schadenverhütung GmbH

Amsterdamer Str. 172-174

D-50735 Köln

Telefon: (0221) 77 66 0; Fax: (0221) 77 66 341

Copyright by VdS Schadenverhütung GmbH. Alle Rechte vorbehalten.

VdS-Richtlinien für die Informationsverarbeitung

Informationssicherheits- managementsystem für kleine und mittlere Unternehmen (KMU)

Anforderungen

Das vorliegende Dokument ist nur verbindlich, sofern dessen Verwendung im Einzelfall vereinbart wird; ansonsten ist die Berücksichtigung dieses Dokuments unverbindlich. Die Vereinbarung zur Verwendung dieses Dokuments ist rein fakultativ. Dritte können im Einzelfall auch andere Anforderungen nach eigenem Ermessen akzeptieren, die diesem Dokument nicht entsprechen.

Inhalt

1	Allgemeines	6
1.1	Anwendungshinweise	6
1.2	Anwendungs- und Geltungsbereich	6
1.3	Gültigkeit	6
2	Normative Verweise	7
3	Begriffe	7
4	Organisation der Informationssicherheit	12
4.1	Verantwortlichkeiten	12
4.1.1	Zuweisung und Dokumentation	12
4.1.2	Funktionstrennungen	12
4.1.3	Zeitliche Ressourcen	12
4.1.4	Delegieren von Aufgaben	13
4.2	Topmanagement	13
4.3	Informationssicherheitsbeauftragter (ISB)	13
4.4	Informationssicherheitsteam (IST)	13
4.5	IT-Verantwortliche	14
4.6	Administratoren	14
4.7	Vorgesetzte	14
4.8	Mitarbeiter	14
4.9	Projektverantwortliche	14
4.10	Externe	15
5	Leitlinie zur Informationssicherheit (IS-Leitlinie)	15
5.1	Allgemeine Anforderungen	15
5.2	Inhalte	15
6	Richtlinien zur Informationssicherheit (IS-Richtlinien)	15
6.1	Allgemeine Anforderungen	15
6.2	Inhalte	16
6.3	Regelungen für Nutzer	16
6.4	Weitere Regelungen	17

7	Mitarbeiter	17
7.1	Vor Aufnahme der Tätigkeit	17
7.2	Aufnahme der Tätigkeit	17
7.3	Beendigung oder Wechsel der Tätigkeit	18
8	Wissen	18
8.1	Aktualität des Wissens	18
8.2	Schulung und Sensibilisierung	18
9	Identifizieren kritischer IT-Ressourcen	19
9.1	Prozesse	19
9.2	Informationen	19
9.3	IT-Ressourcen	20
10	IT-Systeme	21
10.1	Inventarisierung	21
10.2	Lebenszyklus	21
10.2.1	Inbetriebnahme und Änderung	21
10.2.2	Ausmusterung und Wiederverwendung	22
10.3	Basisschutz	22
10.3.1	Software	22
10.3.2	Beschränkung des Netzwerkverkehrs	22
10.3.3	Protokollierung	23
10.3.4	Externe Schnittstellen und Laufwerke	23
10.3.5	Schadsoftware	23
10.3.6	Starten von fremden Medien	23
10.3.7	Authentifizierung	24
10.3.8	Zugänge und Zugriffe	24
10.4	Zusätzliche Maßnahmen für mobile IT-Systeme	24
10.4.1	IS-Richtlinie	24
10.4.2	Schutz der Informationen	25
10.4.3	Verlust	25
10.5	Zusätzliche Maßnahmen für kritische IT-Systeme	25
10.5.1	Risikoanalyse und -behandlung	25
10.5.2	Notbetriebsniveau	25
10.5.3	Robustheit	26
10.5.4	Externe Schnittstellen und Laufwerke	26
10.5.5	Änderungsmanagement	26
10.5.6	Dokumentation	26
10.5.7	Datensicherung	26
10.5.8	Überwachung	26
10.5.9	Ersatzsysteme und -verfahren	27
10.5.10	Kritische Individualsoftware	27
11	Netzwerke und Verbindungen	27
11.1	Netzwerkplan	27
11.2	Aktive Netzwerkkomponenten	27
11.3	Netzübergänge	27
11.4	Basisschutz	28
11.4.1	Netzwerkanschlüsse	28
11.4.2	Segmentierung	28
11.4.3	Fernzugang	29
11.4.4	Netzwerkkopplung	29
11.5	Zusätzliche Maßnahmen für kritische Verbindungen	29

12	Mobile Datenträger	29
12.1	IS-Richtlinie	29
12.2	Schutz der Informationen	30
12.3	Zusätzliche Maßnahmen für kritische mobile Datenträger	30
13	Umgebung	30
13.1	Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen	30
13.2	Datenleitungen	30
13.3	Zusätzliche Maßnahmen für kritische IT-Systeme	31
14	IT-Outsourcing und Cloud Computing	31
14.1	IS-Richtlinie	31
14.2	Vorbereitung	31
14.3	Vertragsgestaltung	31
14.4	Zusätzliche Maßnahmen für kritische IT-Ressourcen	32
15	Zugänge und Zugriffsrechte	33
15.1	Verwaltung	33
15.2	Zusätzliche Maßnahmen für kritische IT-Systeme und Informationen	33
16	Datensicherung und Archivierung	33
16.1	IS-Richtlinie	33
16.2	Archivierung	34
16.3	Verfahren	34
16.4	Weiterentwicklung	34
16.5	Basisschutz	34
16.5.1	Speicherorte	35
16.5.2	Server	35
16.5.3	Aktive Netzwerkkomponenten	35
16.5.4	Mobile IT-Systeme	35
16.6	Zusätzliche Maßnahmen für kritische IT-Systeme	35
16.6.1	Risikoanalyse	35
16.6.2	Verfahren	35
17	Störungen und Ausfälle	35
17.1	IS-Richtlinie	36
17.2	Reaktion	36
17.3	Zusätzliche Maßnahmen für kritische IT-Systeme	36
17.3.1	Wiederanlaufpläne	37
17.3.2	Abhängigkeiten	37
18	Sicherheitsvorfälle	37
18.1	IS-Richtlinie	37
18.2	Erkennen	38
18.3	Reaktion	38
Anhang A	Anhang	39
A.1	Verfahren	39
A.2	Risikoanalyse und -behandlung	39
A.2.1	Risikoanalyse	39
A.2.2	Risikobehandlung	39
A.2.3	Wiederholung und Anpassung	40
Anhang B	Register der Änderungen gegenüber der Vorgängerversion VdS 3473 : 2015-07 (01)	41