Lizenzbestimmungen

4. Kommentierung der VdS 10000 (public)

Die Seiten dieses Bereiches sollen Ihnen nur einen Eindruck vermitteln, welche Inhalte wir für Sie erarbeitet haben. **Deshalb sind die Inhalte absichtlich „verpixelt“**: mehr und mehr Buchstaben werden auf jeder Seite durch Punkte ersetzt.
Wenn Sie auf alle Inhalte zugreifen möchten, benötigen Sie eine entsprechenden Zugang.

Sie möchten einen Zugang erwerben? Hier finden Sie alle weiteren Informationen!

In diesem Bereich finden Sie eine Kommentierung der VdS 10000. Die Kommentierung erläutert die einzelnen Texte, Definitionen, Normative Verwwise, Empfehlungen und Maßnahmen der VdS 10000. Sie richtet sich an Organisationen und Berater, die sich mit der VdS 10000 vertraut machen wollen und dient darüber hinaus als Nachschlagewerk bei Fragen rund um die Implementierung der Richtlinie.

Die unterschiedlichen Inhalte der VdS 10000 sind in der Kommentierung gekennzeichnet:

Anzahl	Art	Gekennzeichnet in der Kommentierung mit
62	Texte	Txxx
75	Definitionen von Begriffen (Kapitel 3)	Dxxx
13	Normative Verweise (Kapitel 2)	Vxxx
Maßnahmen		
91	Grundanforderungen	Gxxx
33	Basisschutz-Maßnahmen	Bxxx
42	Zusätzliche Maßnahmen für kritische Teile der IT-Infrastruktur	Zxxx
68	Empfehlungen	Exxx

Die unterschiedlichen Maßnahmen

Die VdS 10000 beinhalten drei unterschiedlichen Arten von Maßnahmen.

Grundanforderungen (Gxxx)

Grundanforderungen sind Maßnahmen, die immer umgesetzt werden müssen.

Sie sind in den Kapiteln 1, 4 bis 9 und 18, in den Abschnitten 10.1, 10.2, 10.4, 11.1 bis 11.3, 12.1 und 12.2, 13.1 und 13.2, 14.1 bis 14.3, 15.1, 16.1 bis 16.4, 17.1 und 17.2 sowie in den Anhängen A 1 und A2 zu finden.

Maßnahmen des Basisschutzes (Bxxx)

Die Maßnahmen des Basisschutzes müssen nur umgesetzt werden, wenn die betroffenen Teile der IT-Infrastruktur technisch dazu in der Lage sind. Wenn eine Maßnahme des Basisschutzes nicht umgesetzt werden kann, empfehlen die VdS 10000 die Durchführung einer Risikoanalyse und -

behandlung mit der Fragestellung: „Welche Risiken entstehen der Organisation, weil die Maßnahme nicht umgesetzt werden kann?“ Darüber hinaus kann sich die Organisation nach Belieben gegen die Umsetzung jeder einzelnen Maßnahme des Basisschutzes entscheiden (diese Maßnahmen können vermieden werden). Die Ablehnung einer Maßnahme des Basisschutzes verlangt die Durchführung einer entsprechenden Risikoanalyse und -behandlung mit der Fragestellung: „Welche Risiken entstehen der Organisation, weil die Maßnahme nicht umgesetzt wird?“

Die Maßnahmen des Basisschutzes sind in den Abschnitten 10.3.1 bis 10.3.8 (IT-Systeme) 11.4.1 bis 11.4.4 (Netzwerke und Verbindungen) sowie 16.5.1 bis 16.5.4 (Datensicherung und Archivierung) zu finden.

Zusätzliche Maßnahmen für kritische Teile der IT-Infrastruktur (Zxxx)

Die zusätzlichen Maßnahmen für kritische IT-Ressourcen müssen umgesetzt werden, auch wenn dies mit der vorhandenen IT-Infrastruktur nicht möglich ist. Die Organisation muss ggf. die notwendigen Anpassungen an der IT-Infrastruktur vornehmen.

Eine Ausnahme stellen die zusätzlichen Maßnahmen für kritische IT-Systeme (Abschnitte 10.5.1 bis 10.5.10) dar. Bei ihnen kann sich die Organisation nach Belieben gegen ihre Umsetzung entscheiden. Die Ablehnung einer Maßnahme verlangt die Durchführung einer entsprechenden Risikoanalyse und -behandlung mit der Fragestellung: „Welche Risiken entstehen der Organisation, weil die Maßnahme nicht umgesetzt wird?“

Die zusätzlichen Maßnahmen für kritische Teile der IT-Infrastruktur sind in den Abschnitten 10.5.1 bis 10.5.10 (IT-Systeme), 11.5 (Netzwerke), 12.3 (Mobile Datenträger) und 13.3 (Umgebung), 14.4 (IT-Outsourcing und Cloud Computing), 15.2 (Zugänge und Zugriffsrechte), 16.6 (Datensicherung und Archivierung) und 17.3 (Störungen und Ausfälle) zu finden.

Übersicht

Abschnitt	Art der Inhalte T	D	V	G	B	Z	E
0 VdS-Richtlinien für die Informationsverarbeitung	T	-	-	-	-	-	-
1 Allgemeines	T	-	-	-	-	-	-
1.1 Anwendungshinweise	T	-	-	-	-	-	E
1.2 Anwendungs- und Geltungsbereich	T	-	-	-	-	-	E
1.3 Gültigkeit	T	-	-	-	-	-	-
2 Normative Verweise	T	-	V	-	-	-	-
3 Begriffe	-	D	-	-	-	-	-
4 Organisation der Informationssicherheit	T	-	-	-	-	-	-
4.1 Verantwortlichkeiten	-	-	-	G	-	-	-
4.1.1 Zuweisung und Dokumentation	-	-	-	G	-	-	-
4.1.2 Funktionstrennungen	-	-	-	G	-	-	E
4.1.3 Zeitliche Ressourcen	-	-	-	G	-	-	-
4.1.4 Delegieren von Aufgaben	-	-	-	G	-	-	E
4.2 Topmanagement	-	-	-	G	-	-	-
4.3 Informationssicherheitsbeauftragter (ISB)	-	-	-	G	-	-	E

Abschnitt	Art der Inhalte T	D	V	G	B	Z	E
4.4 Informationssicherheitsteam (IST)	-	-	-	G	-	-	-
4.5 IT -Verantwortliche	-	-	-	G	-	-	-
4.6 Administratoren	-	-	-	G	-	-	-
4.7 Vorgesetzte	-	-	-	G	-	-	-
4.8 Mitarbeiter	-	-	-	G	-	-	-
4.9 Projektverantwortliche	-	-	-	G	-	-	-
4.10 Externe	-	-	-	G	-	-	-
5 Leitlinie zur Informationssicherheit (IS-Leitlinie)	T	-	-	-	-	-	-
5.1 Allgemeine Anforderungen	-	-	-	G	-	-	-
5.2 Inhalte	-	-	-	G	-	-	E
6 Richtlinien zur Informationssicherheit (IS-Richtlinien)	T	-	-	-	-	-	-
6.1 Allgemeine Anforderungen	-	-	-	G	-	-	E
6.2 Inhalte	-	-	-	G	-	-	E
6.3 Regelungen für Nutzer	-	-	-	G	-	-	E
6.4 Weitere Regelungen	-	-	-	G	-	-	-
7 Mitarbeiter	T	-	-	-	-	-	-
7.1 Vor Aufnahme der Tätigkeit	-	-	-	G	-	-	-
7.2 Aufnahme der Tätigkeit	-	-	-	G	-	-	-
7.3 Beendigung oder Wechsel der Tätigkeit	-	-	-	G	-	-	-
8 Wissen	T	-	-	-	-	-	-
8.1 Aktualität des Wissens	-	-	-	G	-	-	E
8.2 Schulung und Sensibilisierung	-	-	-	G	-	-	E
9 Identifizieren kritischer IT -Ressourcen	-	-	-	G	-	-	E
9.1 Prozesse	-	-	-	G	-	-	-
9.2 Informationen	-	D	-	G	-	-	E
9.3 IT -Ressourcen	-	D	-	G	-	-	E
10 IT -Systeme	T	-	-	-	-	-	-
10.1 Inventarisierung	-	-	-	G	-	-	E
10.2 Lebenszyklus	T	-	-	-	-	-	-
10.2.1 Inbetriebnahme und Änderung	-	-	-	G	-	-	-
10.2.2 Ausmusterung und Wiederverwendung	-	-	-	G	-	-	-
10.3 Basisschutz	-	-	-	-	B	-	E
10.3.1 Software	-	-	-	-	B	-	E
10.3.2 Beschränkung des Netzwerkverkehrs	-	-	-	-	B	-	E
10.3.3 Protokollierung	-	-	-	-	B	-	E
10.3.4 Externe Schnittstellen und Laufwerke	-	-	-	-	-	-	E
10.3.5 Schadsoftware	-	-	-	-	B	-	E
10.3.6 Starten von fremden Medien	-	-	-	-	B	-	E
10.3.7 Authentifizierung	-	-	-	-	B	-	E
10.3.8 Zugänge und Zugriffe	-	-	-	-	B	-	E
10.4 Zusätzliche Maßnahmen für mobile IT -Systeme	T	-	-	G	-	-	-
10.4.1 IS-Richtlinie	-	-	-	G	-	-	-
10.4.2 Schutz der Informationen	-	-	-	G	-	-	E
10.4.3 Verlust	-	-	-	G	-	-	-

Abschnitt	Art der Inhalte T	D	V	G	B	Z	E
10.5 Zusätzliche Maßnahmen für kritische IT -Systeme	-	-	-	-	-	Z	-
10.5.1 Risikoanalyse und -behandlung	-	-	-	-	-	Z	-
10.5.2 Notbetriebsniveau	-	-	-	-	-	-	E
10.5.3 Robustheit	-	-	-	-	-	Z	-
10.5.4 Externe Schnittstellen und Laufwerke	-	-	-	-	-	Z	-
10.5.5 Änderungsmanagement	-	-	-	-	-	Z	-
10.5.6 Dokumentation	-	-	-	-	-	Z	-
10.5.7 Datensicherung	-	-	-	-	-	Z	-
10.5.8 Überwachung	-	-	-	-	-	Z	E
10.5.9 Ersatzsysteme und -verfahren	-	-	-	-	-	Z	E
10.5.10 Kritische Individualsoftware	-	-	-	-	-	Z	-
11 Netzwerke und Verbindungen	T	-	-	-	-	-	-
11.1 Netzwerkplan	-	-	-	G	-	-	-
11.2 Aktive Netzwerkkomponenten	-	-	-	G	-	-	-
11.3 Netzübergänge	-	-	-	G	-	-	E
11.4 Basisschutz	-	-	-	-	B	-	E
11.4.1 Netzwerkanschlüsse	-	-	-	-	B	-	E
11.4.2 Segmentierung	-	-	-	-	B	-	-
11.4.3 Fernzugang	-	-	-	-	B	-	E
11.4.4 Netzwerkkopplung	-	-	-	-	B	-	-
11.5 Zusätzliche Maßnahmen für kritische Verbindungen	-	-	-	-	-	Z	-
12 Mobile Datenträger	T	-	-	-	-	-	-
12.1 IS-Richtlinie	-	-	-	G	-	-	-
12.2 Schutz der Informationen	-	-	-	-	-	-	E
12.3 Zusätzliche Maßnahmen für kritische mobile Datenträger	-	-	-	-	-	Z	-
13 Umgebung	-	-	-	G	-	-	E
13.1 Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen	-	-	-	G	-	-	E
13.2 Datenleitungen	-	-	-	G	-	-	E
13.3 Zusätzliche Maßnahmen für kritische IT -Systeme	-	-	-	-	-	Z	E
14 IT -Outsourcing und Cloud Computing	T	-	-	-	-	-	-
14.1 IS-Richtlinie	-	-	-	G	-	-	-
14.2 Vorbereitung	-	-	-	G	-	-	-
14.3 Vertragsgestaltung	-	-	-	G	-	-	E
14.4 Zusätzliche Maßnahmen für kritische IT -Ressourcen	-	-	-	-	-	Z	E
15 Zugänge und Zugriffsrechte	T	-	-	-	-	-	-
15.1 Verwaltung	-	-	-	G	-	-	E
15.2 Zusätzliche Maßnahmen für kritische IT -Systeme und Informationen	-	-	-	-	-	Z	-
16 Datensicherung und Archivierung	T	-	-	G	-	-	E
16.1 IS-Richtlinie	-	-	-	G	-	-	-
16.2 Archivierung	-	-	-	G	-	-	-
16.3 Verfahren	-	-	-	G	-	-	E
16.4 Weiterentwicklung	-	-	-	G	-	-	-
16.5 Basisschutz	-	-	-	-	B	-	E
16.5.1 Speicherorte	-	-	-	-	B	-	-

Abschnitt	Art der Inhalte T	D	V	G	B	Z	E
16.5.2 Server	-	-	-	-	B	-	-
16.5.3 Aktive Netzwerkkomponenten	-	-	-	-	B	-	-
16.5.4 Mobile IT -Systeme	-	-	-	-	B	-	-
16.6 Zusätzliche Maßnahmen für kritische IT -Systeme	-	-	-	-	-	Z	-
16.6.1 Risikoanalyse	-	-	-	-	-	Z	-
16.6.2 Verfahren	-	-	-	-	-	Z	-
17 Störungen und Ausfälle	T	-	-	G	-	-	E
17.1 IS-Richtlinie	-	-	-	G	-	-	E
17.2 Reaktion	-	-	-	G	-	-	E
17.3 Zusätzliche Maßnahmen für kritische IT -Systeme	-	-	-	-	-	Z	-
17.3.1 Wiederanlaufpläne	-	-	-	-	-	Z	-
17.3.2 Abhängigkeiten	-	-	-	-	-	Z	E
18 Sicherheitsvorfälle	T	-	-	-	-	-	-
18.1 IS-Richtlinie	-	-	-	G	-	-	E
18.2 Erkennen	-	-	-	-	-	-	E
18.3 Reaktion	-	-	-	G	-	-	E
Anhang A	-	-	-	-	-	-	-
A 1 Verfahren	-	-	-	G	-	-	E
A 2 Risikoanalyse und -behandlung	-	-	-	G	-	-	E
A 2.1 Risikoanalyse	-	-	-	G	-	-	-
A 2.2 Risikobehandlung	-	-	-	G	-	-	-
A 2.3 Wiederholung und Anpassung	-	-	-	G	-	-	-
Anhang B Register der Änderungen gegenüber der Vorgängerversion VdS 3473 : 2015-07 (01)	T	-	-	-	-	-	-

Wenn Sie eine (ausführlichere) Kommentierung einer Maßnahme wünschen, Sie uns Lob oder Kritik übermitteln möchten, so steht Ihnen am Ende jeder Seite ein Feedback-Formular zur Verfügung.