 © 2016 by 3473 Gurus GbR

Lizenzbestimmungen

• Diese Materialien sind lizenziert für @USERINFONAME@.
• Die Materialien dürfen **ausschließlich** für die Implementation, Verbesserung oder den Betrieb von Sicherheitsmaßnahmen innerhalb der genannten Organisation genutzt werden.
• Hierfür dürfen die Materialien beliebig verändert, ergänzt oder neu gestaltet werden.
• Für alle anderen Einsatzzwecke - insbesondere für die Veröffentlichung der Materialien und deren Einsatz für Kunden des Lizenznehmers - muss im Vorfeld eine schriftliche Genehmigung der 3473 Gurus GbR eingeholt bzw. eine entdprechende Lizenz erworben werden.

 © 2016 by 3473 Gurus GbR

Analyse: Anpassung/Ergänzung der VdS 10000

Es kristallisiert sich immer mehr heraus, dass die VdS 10000 ein optimaler Ausgangspunkt für die Umsetzung von NIS-2 ist. Die Anforderungen des NIS2UmsuCG können an den folgenden Stellen in die VdS 10000 integriert werden:

Text der VdS 10000	**Vorgaben des BSIG im NIS2UmsuCG**	**Erläuterung/Anmerkung**
1 Allgemeines		
1.1 Anwendungshinweise		
1.2 Anwendungs- und Geltungsbereich	§ 28 Besonders wichtige Einrichtungen und wichtige Einrichtungen	Verfahren: Analyse vorschreiben.
	§ 33 Registrierungspflicht	Teil des Verfahrens „Analyse“: Betroffene müssen sich registrieren.
	§ 34 Besondere Registrierungspflicht für bestimmte Einrichtungsarten	Teil des Verfahrens „Analyse“: Bestimmte Einrichtungen müssen weitere Angaben machen
1.3 Gültigkeit		
2 Normative Verweise		
3 Begriffe	§2 Begriffsbestimmungen	
4 Organisation der Informationssicherheit		
4.1 Verantwortlichkeiten		
4.1.1 Zuweisung und Dokumentation		
4.1.2 Funktionstrennungen		
4.1.3 Zeitliche Ressourcen		
4.1.4 Delegieren von Aufgaben		
4.2 Topmanagement	§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Reporting stärken.
	§ 38 Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Schulung
4.3 Informationssicherheitsbeauftragter (ISB)	§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Reporting stärken.

 © 2016 by 3473 Gurus GbR

Text der VdS 10000	Vorgaben des BSIG im NIS2UmsuCG	Erläuterung/Anmerkung
4.4 Informationssicherheitsteam (IST)	§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Reporting stärken.
4.5 IT-Verantwortliche		
4.6 Administratoren		
4.7 Vorgesetzte		
4.8 Mitarbeiter		
4.9 Projektverantwortliche		
4.10 Externe		
5 Leitlinie zur Informationssicherheit (IS-Leitlinie)		
5.1 Allgemeine Anforderungen		
5.2 Inhalte		
6 Richtlinien zur Informationssicherheit (IS-Richtlinien)		
6.1 Allgemeine Anforderungen		
6.2 Inhalte		
6.3 Regelungen für Nutzer		
6.4 Weitere Regelungen		
7 Mitarbeiter		
7.1 Vor Aufnahme der Tätigkeit		
7.2 Aufnahme der Tätigkeit		
7.3 Beendigung oder Wechsel der Tätigkeit		
8 Wissen		
8.1 Aktualität des Wissens	§ 5 Allgemeine Meldestelle für die Sicherheit in der Informationstechnik	
	§ 6 Informationsaustausch	Nutzen des Informationsaustausches
	§ 13 Warnungen	Warnungen des BSi erwähnen und Reaktion erfordern.
8.2 Schulung und Sensibilisierung	§ 38 Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Schulungspflicht für Topmanagement aufnehmen.
9 Identifizieren kritischer IT-Ressourcen		

Text der VdS 10000	Vorgaben des BSIG im NIS2UmsuCG	Erläuterung/Anmerkung
9.1 Prozesse	§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Ermitteln der schützenswerten Ressourcen
	§ 38 Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Billigung expliziter formulieren bzw. verankern.
9.2 Informationen	§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Ermitteln der schützenswerten Ressourcen
	§ 38 Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Billigung expliziter formulieren bzw. verankern.
9.3 IT-Ressourcen	§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Ermitteln der schützenswerten Ressourcen
	§ 38 Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Billigung expliziter formulieren bzw. verankern.
10 IT-Systeme		
10.1 Inventarisierung		
10.2 Lebenszyklus		
10.2.1 Inbetriebnahme und Änderung		
10.2.2 Ausmusterung und Wiederverwendung		
10.3 Basisschutz	§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Risikobasierter Ansatz und „Stand der Technik“ stärken.
10.3.1 Software		
10.3.2 Beschränkung des Netzwerkverkehrs		
10.3.3 Protokollierung	§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Auswertung von Logmeldungen vorschreiben.
10.3.4 Externe Schnittstellen und Laufwerke		

 © 2016 by 3473 Gurus GbR

Text der VdS 10000	Vorgaben des BSIG im NIS2UmsuCG	Erläuterung/Anmerkung
10.3.5 Schadsoftware		
10.3.6 Starten von fremden Medien		
10.3.7 Authentifizierung		
10.3.8 Zugänge und Zugriffe		
10.4 Zusätzliche Maßnahmen für mobile IT-Systeme		
10.4.1 IS-Richtlinie		
10.4.2 Schutz der Informationen		
10.4.3 Verlust		
10.5 Zusätzliche Maßnahmen für kritische IT-Systeme		
10.5.1 Risikoanalyse und -behandlung		
10.5.2 Notbetriebsniveau		
10.5.3 Robustheit		
10.5.4 Externe Schnittstellen und Laufwerke		
10.5.5 Änderungsmanagement		
10.5.6 Dokumentation		
10.5.7 Datensicherung		
10.5.8 Überwachung		
10.5.9 Ersatzsysteme und -verfahren		
10.5.10 Kritische Individualsoftware		
11 Netzwerke und Verbindungen		
11.1 Netzwerkplan		
11.2 Aktive Netzwerkkomponenten		
11.3 Netzübergänge		
11.4 Basisschutz	§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Risikobasierter Ansatz und „Stand der Technik“ stärken.
11.4.1 Netzwerkanschlüsse		
11.4.2 Segmentierung		
11.4.3 Fernzugang		
11.4.4 Netzwerkkopplung		
11.5 Zusätzliche Maßnahmen für kritische Verbindungen		
12 Mobile Datenträger		
12.1 IS-Richtlinie		
12.2 Schutz der Informationen		
12.3 Zusätzliche Maßnahmen für kritische mobile Datenträger		
13 Umgebung		
13.1 Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen		

Text der VdS 10000	Vorgaben des BSIG im NIS2UmsuCG	Erläuterung/Anmerkung
13.2 Datenleitungen		
13.3 Zusätzliche Maßnahmen für kritische IT-Systeme		
14 IT-Outsourcing und Cloud Computing	§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Lieferkette
14.1 IS-Richtlinie		
14.2 Vorbereitung		
14.3 Vertragsgestaltung		
14.4 Zusätzliche Maßnahmen für kritische IT-Ressourcen		
15 Zugänge und Zugriffsrechte		
15.1 Verwaltung		
15.2 Zusätzliche Maßnahmen für kritische IT-Systeme und Informationen		
16 Datensicherung und Archivierung		
16.1 IS-Richtlinie		
16.2 Archivierung		
16.3 Verfahren		
16.4 Weiterentwicklung		
16.5 Basisschutz	§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Risikobasierter Ansatz und „Stand der Technik“ stärken.
16.5.1 Speicherorte		
16.5.2 Server		
16.5.3 Aktive Netzwerkkomponenten		
16.5.4 Mobile IT-Systeme		
16.6 Zusätzliche Maßnahmen für kritische IT-Systeme		
16.6.1 Risikoanalyse		
16.6.2 Verfahren		
17 Störungen und Ausfälle		
17.1 IS-Richtlinie		
17.2 Reaktion	§ 11 Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen	In Verfahren aufnehmen: Unterstützung durch BSI prüfen
	§ 32 Meldepflichten	Meldungen in die Bewältigung eines Vorfalls aufnehmen.
17.3 Zusätzliche Maßnahmen für kritische IT-Systeme		

Text der VdS 10000	Vorgaben des BSIG im NIS2UmsuCG	Erläuterung/Anmerkung
17.3.1 Wiederanlaufpläne		
17.3.2 Abhängigkeiten		
18 Sicherheitsvorfälle		
18.1 IS-Richtlinie		
18.2 Erkennen	§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Auswertung von Logmeldungen vorschreiben.
18.3 Reaktion	§ 11 Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen	In Verfahren aufnehmen: Unterstützung durch BSI prüfen
	§ 32 Meldepflichten	Betroffenen müssen Erstmeldung, erste Bewertung, Zwischenmeldung und Abschlussmeldung abgeben → in Verfahren aufnehmen
	§ 35 Unterrichtungspflichten	Einrichtungen müssen u. U. Betroffene informieren → in Verfahren aufnehmen.
Anhang A Anhang		
A.1 Verfahren		
A.2 Risikoanalyse und -behandlung		
A.2.1 Risikoanalyse	§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Vorgehensweisen RA. Auswahl der Maßnahmen. Dokumentation.
	§ 38 Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Billigung verankern.
A.2.2 Risikobehandlung	§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Vorgehensweise RB. Umsetzung der Maßnahmen. Prüfung. Dokumentation.
	§ 38 Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Billigung verankern.

Text der VdS 10000	Vorgaben des BSIG im NIS2UmsuCG	Erläuterung/Anmerkung
A.2.3 Wiederholung und Anpassung	§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	
	§ 38 Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	Billigung verankern.

Ich möchte...
...etwas in diesem Artikel kommentieren.☐
Ihre Kontaktdaten (für Rückfragen, optional)

Only edit this fieldset if "...etwas in diesem Artikel kommentieren." is set.

Name (optional) Ihre Mailadresse (optional)
Wir möchten wissen, dass Sie ein Mensch sind

Only edit this fieldset if "...etwas in diesem Artikel kommentieren." is set.

Geben Sie hier die Zahl 'zwanzig minus elf' als Ziffer ein. *
Ihr Feedback

Only edit this fieldset if "...etwas in diesem Artikel kommentieren." is set.

Wie finden Sie diesen Artikel? * bitte wählen
Was fanden Sie besonders gut? (optional)

Only edit this fieldset if "...etwas in diesem Artikel kommentieren." is set.

Was sollte besser werden? (optional)

Only edit this fieldset if "...etwas in diesem Artikel kommentieren." is set.

Only edit this fieldset if "...etwas in diesem Artikel kommentieren." is set.

Feedback absenden