
Inhaltsverzeichnis

1	Einleitung	1
1.1	NIS-2: Betroffene Einrichtungen	3
1.1.1	Sektor Gesundheit	3
1.1.1.1	Primärversorger	4
1.1.1.2	Lieferketten Betroffene	4
1.1.2	Alle Sektoren außerhalb des Gesundheitssektors	5
1.2	Zahlen, Fakten und Marktdaten (Stand 2025)	6
1.3	Definitionen	7
2	Einführung zu NIS-2	11
2.1	Risikobewertungen und Sicherheitsrichtlinien	12
2.2	Bewertung der Wirksamkeit von Sicherheitsmaßnahmen	12
2.3	Einsatz von Kryptographie und Verschlüsselung	12
2.4	Umgang mit Sicherheitsvorfällen	12
2.5	Beschaffung von Systemen	13
2.6	Sicherheit im Zusammenhang mit Lieferketten	13
2.7	Cybersicherheitsschulungen und Computerhygiene	13
2.8	Sicherheitsverfahren für Zugang zu sensiblen Daten	13
2.9	Geschäftsbetrieb während und nach einem Sicherheitsvorfall	14
2.10	Einsatz von Multifaktor-Authentifizierung	14
2.11	Zusammenfassung zur Anwendung von NIS-2	14
3	Leitlinien zur Informationssicherheit (NIS-2 kompatibel)	15
3.1	Grundlagen	15
3.1.1	Ausgangspunkt	16
3.1.2	Verantwortlichkeit	16
3.1.3	Anwendungsbereich	17
3.2	Bedeutung des ISMS	17

3.3	Ziele und Strategie	18
3.3.1	Definition der Ziele	18
3.3.2	Strategie zur Zielerreichung	18
3.3.3	Risikomanagement	19
3.3.4	Verantwortlichkeit der Leitung	19
3.3.5	Berichtspflichten	19
3.3.6	Versorgungskontinuität	20
3.4	Management und Organisation	20
3.4.1	Management	20
3.4.2	Organisationsstrukturen.	21
4	Maßnahmen- und Aufgabenplanung der Abteilungen	23
4.1	Geschäftsleitung.	23
4.2	Rechtsabteilung	24
4.3	Personalabteilung.	25
4.4	Einkaufsabteilung	25
4.5	IT-Abteilung.	26
4.6	QM-Abteilung/Sicherheitsabteilung	26
4.7	Finanzabteilung und Verwaltung	27
4.8	Versorgungsabteilungen (ambulant oder stationär)	28
5	PDCA: Kontinuierlicher Verbesserungsprozess des ISMS	29
5.1	Planungsprozess.	30
5.2	Umsetzungsprozess	30
5.3	Evaluierungsprozess.	31
5.4	Korrekturprozess	31
6	Konsolidierte Assistenzsysteme (KAS)	33
7	Lieferanten und Partner.	37
7.1	NIS2 Lieferanten Onboarding	37
7.2	Lieferanten Monitoring (Lieferketten).	38
7.2.1	Beispiele für typische Störfälle in der Lieferkette.	38
7.2.2	Beispiel einer Verfahrensanweisung für Lieferkettenmonitoring	38
8	NIS-2 Planung	43
8.1	ISMS-Status, Standards und Normen	43
8.1.1	ISO 27001	45
8.1.2	B3S	45
8.1.3	VdS 10000.	46

8.1.4	DIN ES 15224	46
8.1.5	ISO 9001 mit IS- Ergänzung	46
8.1.6	ISO 27799	46
8.1.7	BSI-Grundsatz	47
8.1.8	ISMS-Eigenentwicklung	47
8.1.9	Industrie und Gruppen-ISMS	47
8.2	Zeit und Kostenplanung	47
8.3	NIS-2 Schulungsplanung	48
8.3.1	Schulung für die Geschäftsleitung	48
8.3.2	Schulung für das Management und Beauftragte	49
8.3.3	Schulung für Mitarbeitende	50
8.4	Curriculum	50
8.5	Key Risk Indicators (KRI)	52
8.6	PDCA und Optimierungsmanagement	53
9	Ausblick	55
10	Empfehlungen	57
11	Anhang	59
11.1	B3S (Verfahrensweisung zum ISMS-Plan)	59
11.2	NIS-2 Kernprozesse der Abteilungen (Mitgeltende NIS-2 Prozesse)	62
11.3	NIS-2 Projektplan Krankenhaus (Beispiel)	66
	Was Sie aus diesem <i>essential</i> mitnehmen können	69
	Glossar	71
	Literatur	75