A1 Digital
NIS Checkliste

A1 Digital

NIS Verordnung Checkliste

Nr.	Titel	Maßnahme	Habe ich...?	Status	Notizen
1.	**Governance und Risikomanagement**				
1.1	**Risikoanalyse:**	Eine Risikoanalyse der Netz- und Informationssysteme ist durchzuführen. Dabei sind spezifische Risiken auf Grundlage einer Analyse der betrieblichen Auswirkungen von Sicherheitsvorfällen zu ermitteln und hinsichtlich der hohen Bedeutung des Betreibers wesentlicher Dienste für das Funktionieren des Gemeinwesens zu bewerten.	Dokumentierter Prozess der regelmäßige Durchführung der Risikoanalyse definiert		
			Dokumentation der bekannten Informationssicherheits-Risiken in der Organisation		
			Dokumentation dass Ergebnisse der Risikoanalyse der obersten Unternehmensleitung angemessen bekannt gemacht wurden		
1.2	**Sicherheitsrichtlinie:**	Eine Sicherheitsrichtlinie ist zu erstellen und periodisch zu aktualisieren.	Dokumentierte Sicherheitsrichtlinie welche alle NIS-relevanten Systeme und Prozesse umfasst		
			Letzte Aktualisierung nicht älter als 12 Monate		
1.3	**Überprüfungsplan der Netz- und Informationssysteme:**	Die Durchführung der periodischen Überprüfung der Netz- und Informationssystemsicherheit ist zu planen und festzulegen.	Dokumentierter Auditplan, der sicherstellt, dass alle NIS-relevanten Systeme und Prozesse regelmäßig auditiert werden		
			Letztes technisches Audit nicht länger als 12 Monate in der Vergangenheit		
			Dokumentation über angemessene Nachverfolgungen von Maßnahmen aus Audits		

1.4	**Ressourcenmanagement:**	Alle Ressourcen, die erforderlich sind, um die Funktionsfähigkeit der Netz- und Informationssysteme zu gewährleisten, sind im Hinblick auf kurz-, mittel- und langfristige Kapazitätsanforderungen einzuplanen und sicherzustellen.	Dokumentierte Informationssicherheitsorganisation mit Verantwortlichkeiten und Ressourcen		
			Dokumentation der IT-Resourcen (IT-Budget)		
1.5	**Informationssicherheits-managementsystemprüfung:**	Die periodische Überprüfung des Informationssicherheits-managementsystems ist festzulegen und durchzuführen.	Dokumentierter Auditplan der sicherstellt, dass alle Vorgaben aus dem ISMS regelmäßig auditiert werden		
			letztes Audit des ISMS nicht länger als 12 Monate in der Vergangenheit		
			Dokumentation über angemessene Nachverfolgungen von Maßnahmen aus Audits		
1.6	**Personalwesen:**	Sicherheitsrelevante Aspekte sind in den Prozessen des Personalwesens zu berücksichtigen und umzusetzen.	Dokumentierte Prozesse für Mitarbeitereintritt, Wechsel und Austritt		
			Mitarbeiter in kritischen Funktionen sind angemessen überprüft vor Einstellung (z.B. polizeiliches Führungszeugnis)		

2. Umgang mit Dienstleistern, Lieferanten und Dritten

2.1	**Beziehungen mit Dienstleistern, Lieferanten und Dritten:**	Anforderungen an Dienstleistern, Lieferanten und Dritte für den Betrieb von, einen sicheren Zugang zu und Zugriff auf Netz- und Informationssysteme sind festzulegen und periodisch zu überprüfen.	Anforderungen an Informationssicherheit sind Vertragsbestandteil bei allen wesentlichen Dienstleistern		
2.2	**Leistungsvereinbarungen mit Dienstleistern und Lieferanten:**	Die Leistungsvereinbarungen mit Dienstleistern und Lieferanten sind periodisch zu überprüfen und zu überwachen.	Leistungen von Dienstleistern werden nachweislich regelmäßig überwacht		
			Abweichungen werden gemäßg einem festgelegten Prozess behandelt.		

3. Sicherheitsarchitektur

3.1	**Systemkonfiguration:**	Netz- und Informationssysteme sind sicher zu konfigurieren. Diese Konfiguratoin ist strukturiert zu dokumentieren. Die Dokumentation ist aktuell zu halten.	Dokumentierter Prozess zur sicheren Konfiguration von Systemen		
			letzte Aktualisierung der Dokumentation darf nicht älter als 12 Monate sein		
			Überprüfungen auf von Vorgaben abweichende oder unsichere Konfigurationen finden statt		
			Abweichungen werden gemäßg einem festgelegten Prozess behandelt.		
3.2	**Vermögenswerte:**	Vermögenswerte, die im Zusammenhang mit Netz- und Informationssystemen stehen, sind strukturiert zu analysieren und zu dokumentieren.	Dokumentierter Prozess zur Identifikation und Klassifikation von Unternehmenswerten (Informationen, IT-Assets)		
			Inventar der Werte ist angemessen (z.B. in einer Datenbank) und aktuell		
3.3	**Netzwerksegmentierung:**	Eine Segmentierung der Netzwerke ist innerhalb der Netz- und Informationssysteme abhängig vom Schutzbedarf vorzunehmen.	Angemessene Dokumentation der Segmentierung (Schutzbedarf, erlaubte Kommunikation zwischen Segmenten, etc.) vorhanden		
			Technische Implementierung wird regelmäßig überprüft		
3.4	**Netzwerksicherheit:**	Die Sicherheit innerhalb der Netzwerksegmente und der Schnittstellen zwischen den Netzwerksegmenten ist zu gewährleisten.	Angemessene Dokumentation der Maßnahmen (z.B. Firewall, IDS/IPS, DLP, etc.) vorhanden		

			Prozess und Tools zur Erkennung von Schwachstellen in Sytemen ist vorhanden (z.B. Schwachstellen-Scanner)		
			Technische Implementierung wird regelmäßig überprüft		
3.5	**Kryptographie:**	Vertraulichkeit, Authentizität und Integrität von Informationen sind durch den angemessenen und wirksamen Einsatz kryptographischer Verfahren und Technologien sicherzustellen.	Angemessene Dokumentation der Maßnahmen (z.B. Verschlüsselung von Speichern, Transportverschlüsselung, Management von Schlüsseln, etc.)		
			Technische Implementierung wird regelmäßig überprüft		

4. Systemadministration

4.1	**Administrative Zugangsrechte:**	Administrative Zugangsrechte sind eingeschränkt nach dem Minimalrechtsprinzip zuzuweisen. Diese Zuweisungen sind periodisch zu überprüfen und gegebenenfalls anzupassen.	Dokumentierte Verwaltungsprozesse für Accounts mit Admin-Rechten (Vergabe, Entzug, geteilte Accounts/ Passwörter, regelmäßige Überprüfung)		
			Vergabe von Zugrangsrechten kann in den Systemen nachgewiesen werden (z.B. Logging)		
			letzte Überprüfung nicht älter als 12 Monate		
4.2	**Systeme und Anwendungen zur Systemadministration:**	Systeme und Anwendungen zur Systemadministration sind ausschließlich für Tätigkeiten zum Zweck der Systemadministration zu verwenden. Die Sicherheit dieser Systeme und Anwendungen ist zu gewährleisten.	Angemessene Trennung von administrativen Accounts und normalen Benutzeraccounts		
			dedizierte Systeme/Anwendungen zur Systemadministration sind angemessen gehärtet		
			Technische Implementierung wird regelmäßig überprüft		

5. Identitäts- und Zugriffsmanagement

5.1	**Identifikation und Authentifikation:**	Es sind Verfahren umzusetzen und Technologien einzusetzen, die die Identifikation und Authentifikation von Benutzern und Diensten gewährleisten.	Dokumentation der Verwaltungsprozesse für Accounts (Vergabe, Änderung, Entzug, regelmäßige Überprüfung), personalisierte Benutzeraccounts vorhanden, dedizierte Accounts für Dienste vorhanden		
			Personen arbeiten nur mit personalisierten Benutzeraccounts		
			Systemdienste verwenden nur dedizierte Accounts		
5.2	**Autorisierung:**	Es sind Verfahren umzusetzen und Technologien einzusetzen, die unautorisierte Zugriffe auf Netz- und Informationssysteme unterbinden.	Angemessene technische Maßnahmen zur Netzwerkauthentifikation (z.B. 802.1X) sind implementiert		
			Angemessene Authentifikationsmethoden für Benutzer sind implementiert (starkes Passwort, Multifaktor, Biometrik, etc.)		
			Passwort-Regeln sind technisch erzwungen		
			Technische Implementierung wird regelmäßig überprüft		

6. Systemwartung und Betrieb

6.1	**Systemwartung und Betrieb:**	Abläufe und Vorgänge zur Gewährleistung eines sicheren Systembetriebs von Netz- und Informationssystemen sind einzuführen und periodisch zu überprüfen.	Dokumentation der Betriebsführungsprozesse vorhanden und nicht älter als 12 Monate		

			Wartungsplan vorhanden und Wartungen wie geplant durchgeführt		
			Security ist Teil des Software-entwicklungsprozesses (z.B. Code-Prüfungen, Abnahme-Tests, etc.)		
6.2	**Fernzugriff:**	Fernzugriff ist eingeschränkt nach dem Minimalrechtsprinzip und zeitlich beschränkt zu vergeben. Die Fern-zugriffsrechte sind periodisch zu überprüfen und gegebenenfalls anzupassen. Die Sicherheit des Fernzugriffs ist zu gewährleisten.	Dokumentation der Verwaltungs-prozesse für Fernzugriffe (Vergabe, Entzug, regelmäßige Überprüfung),		
			letzte Überprüfung nicht älter als 12 Monate		
			Fernzugriffe sind mit angemessener Mehr-Faktor-Authentifizierung (zumindest 2 Faktoren) geschützt		
			Mobile Endgeräte sind angemessen zentral verwaltet und geschützt		

7. Physische Sicherheit

7.1	**Physische Sicherheit:**	Der physische Schutz der Netz- und Informationssysteme, insbesondere der physische Schutz vor unbefugtem Zutritt und Zugang, ist zu gewährleisten.	Dokumentation der Zutrittsverwaltungprozesse (Vergabe, Änderung, Enzug, regelmäßige Über-prüfung, Umgang mit Gästen)		
			physikalische Maßnahmen zum Zu-trittsschutz angemessen: zB. Zäune, vergitterte Fenster, Vereinzelungs-anlage, Videoüberwachung, Wach-dienst, etc.		
			angemessener Schutz vor Elementar-bedrohungen: Feuerlöscher, Wasser-sensoren, Temperatur/Klima geregelt, etc.		

8. Erkennung von Vorfällen

8.1	**Erkennung:**	Mechanismen zur Erkennung und Bewertung von Vorfällen sind umzusetzen.	Prozess zur Meldung von möglichen Sicherheitsvorfällen ist dokumentiert und kommuniziert		
			Prozess zur Prüfung von Logs auf Sicherheitsvorfälle ist dokumentiert (Scope der Systeme, welche Arten von Vorfällen erkannt werden sollen, Verantwortlichkeiten, zeitliche Vorgaben, etc.)		
8.2	**Protokollierung und Monitoring:**	Mechanismen zu Protokollierung und Monitoring, insbesondere von für die Erbringung des wesentlichen Dienstes essentiellen Tätigkeiten und Vorgängen, sind umzusetzen.	Alle relevanten Systeme produzieren Logs		
			alle relevanten Systeme werden in Monitoring überwacht		
8.3	**Korrelation und Analyse:**	Mechanismen zur Erkennung und adäquaten Bewertung von Vorfällen durch die Korrelation und Analyse der ermittelten Protokolldaten sind umzusetzen.	Logs werden zentral gesammelt		
			Use Cases zur Erkennung von möglichen Sicherheitsvorfällen sind dokumentiert und umgesetzt		

9. Bewältigung von Vorfällen

9.1	**Vorfallsreaktion:**	Prozesse zur Reaktion auf Vorfälle sind zu erstellen, aufrechtzuerhalten und zu erproben.	Prozess zur Information Security Incident Management and Response ist vorhanden und dokumentiert		
			Letzte Änderung ist nicht älter als 12 Monate		
			Security Incidents werden gemäß dem Prozess behandelt		
			der letzte Test des Prozesse ist nicht älter als 12 Monate		

9.2	**Vorfallsmeldung:**	Prozesse zur internen und externen Meldung von Vorfällen sind zu erstellen, aufrechtzuerhalten und zu erproben.	Meldeprozesse sind vorhanden und dokumentiert		
			Dokumentation ist nicht älter als 12 Monate		
			der letzte Test der Prozesse ist nicht älter als 12 Monate		
9.3	**Vorfallsanalyse:**	Prozesse zur Analyse und Bewertung von Vorfällen und zur Sammlung relevanter Informationen sind zu erstellen, aufrechtzuerhalten und zu erproben, um den kontinuierlichen Verbesserungsprozess zu fördern.	Prozesse und angemessene Werkzeuge zur Analyse von Vorfällen sind vorhanden und dokumentiert		
			Dokumentation ist nicht älter als 12 Monate		
			der letzte Test der Prozesse ist nicht älter als 12 Monate		

10. Betriebskontinuität

10.1	**Betriebskontinuitäts-management:**	Die Wiederherstellung der Erbringung des wesentlichen Dienstes auf einem zuvor festgelegten Qualitätsniveau nach einem Sicherheitsvorfall ist zu gewährleisten.	Dokumenation von Business Continuity Management ist angemessen – enthält zumindest: Scope, Organisation, Risikobewertung (BIA)		
			Dokumentation ist nicht älter als 12 Monate		
10.2	**Notfallmanagement:**	Notfallpläne sind zu erstellen, anzuwenden, regelmäßig zu bewerten und zu erproben.	Notfallpläne und technische Beschreibungen für Wiederherstellung sind für alle wesentliche Systeme vorhanden		
			letzter Test nicht älter als 12 Monate		

11. Krisenmanagement

11.1	**Krisenmanagement:**	Rahmenbedingungen und Prozess-abläufe des Krisenmanagements sind für die Aufrechterhaltung des wesentlichen Dienstes vor und während eines Sicherheitsvorfalls zu definieren, umzusetzen und zu erproben.	Krisenmanagement und Prozesse sind dokumentiert und organisatorisch verankert		
			Dokumentation nicht älter als 12 Monate		
			letzter Test nicht älter als 12 Monate		

A1 Digital

Kontakt Deutschland
A1 Digital Deutschland GmbH
St.-Martin-Straße 59
81669 München
Deutschland
E-Mail: sales@a1.digital

https://a1.digital

Kontakt Österreich
A1 Digital International GmbH
Lassallestraße 9
1020 Wien
Österreich
E-Mail: info@a1.digital

https://a1.digital

Jetzt Partner werden!
A1 Digital Deutschland GmbH
St.-Martin-Straße 59
81669 München
Deutschland
E-Mail: partnering@a1.digital

https://a1.digital/partner-werden