Statement of Applicability (SoA) – Version 3.0 (Public)

Version	3.0
Veröffentlichungsdatum	28.01.2025
Klassifizierung	Öffentlich
Eigentümer	Informationssicherheitsbeauftragter CGM AT
Status	Final

ISO 27001:2022

Maßnahmen ID (Control ID)	*Maßnahmenbezeichnung (Control Name)*	*Anwendbar (gem. 6.1.3 d)*	** Gründe für die Auswahl von Maßnahmenzielen und Maßnahmen (gem. 6.1.3 d)*		
			CA	*BO*	*RA*
5	**Organisatorische Maßnahmen**				
5.1	Informationssicherheitsrichtlinien	☑	x	x	
5.2	Informationssicherheitsrollen und -verantwortlichkeiten	☑	x	x	
5.3	Aufgabentrennung	☑	x	x	x
5.4	Verantwortlichkeiten der Leitung	☑	x	x	
5.5	Kontakt mit Behörden	☑	x	x	
5.6	Kontakt mit speziellen Interessensgruppen	☑	x	x	
5.7	Bedrohungsintelligenz	☑		x	x
5.8	Informationssicherheit im Projektmanagement	☑	x	x	x
5.9	Inventar der Informationen und anderen damit verbundenen Werten	☑	x	x	x
5.10	Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten	☑		x	x

CompuGroup Medical Österreich
Statement of Applicability (SoA)
Version 3.0 (Public)

Maßnahmen ID (Control ID)	Maßnahmenbezeichnung (Control Name)	Anwendbar (gem. 6.1.3 d)	* Gründe für die Auswahl von Maßnahmenzielen und Maßnahmen (gem. 6.1.3 d)		
			CA	BO	RA
5.11	Rückgabe von Werten	☑	x	x	x
5.12	Klassifizierung von Information	☑	x	x	x
5.13	Kennzeichnung von Information	☑		x	x
5.14	Informationsübertragung	☑	x	x	x
5.15	Zugangssteuerung	☑	x	x	x
5.16	Identitätsmanagement	☑	x	x	x
5.17	Informationen zur Authentifizierung	☑	x		x
5.18	Zugangsrechte	☑			x
5.19	Informationssicherheit in Lieferantenbeziehungen	☑	x	x	x
5.20	Behandlung von Informationssicherheit in Lieferantenvereinbarungen	☑	x	x	x
5.21	Umgang mit der Informationssicherheit in der IKT-Lieferkette	☑	x	x	x
5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	☑			
5.23	Informationssicherheit für die Nutzung von Cloud-Diensten	☑		x	x
5.24	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	☑	x	x	
5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse	☑	x	x	
5.26	Reaktion auf Informationssicherheitsvorfälle	☑	x	x	
5.27	Erkenntnisse aus Informationssicherheitsvorfällen	☑	x		x
5.28	Sammeln von Beweismaterial	☑	x	x	
5.29	Informationssicherheit bei Störungen	☑	x	x	
5.30	IKT-Bereitschaft für Business Continuity	☑	x	x	
5.31	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen	☑	x		
5.32	Geistige Eigentumsrechte	☑	x		
5.33	Schutz von Aufzeichnungen	☑	x		
5.34	Datenschutz und Schutz personenbezogener Daten (pbD)	☑	x		
5.35	Unabhängige Überprüfung der Informationssicherheit	☑	x		

CompuGroup Medical Österreich
Statement of Applicability (SoA)
Version 3.0 (Public)

Maßnahmen ID (Control ID)	Maßnahmenbezeichnung (Control Name)	Anwendbar (gem. 6.1.3 d)	* Gründe für die Auswahl von Maßnahmenzielen und Maßnahmen (gem. 6.1.3 d)		
			CA	BO	RA
5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	☑	x		
5.37	Dokumentierte Betriebsabläufe	☑	x	x	x
6	**Personenbezogene Maßnahmen**				
6.1	Sicherheitsüberprüfung	☑			x
6.2	Beschäftigungs- und Vertragsbedingungen	☑	x	x	
6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung	☑		x	
6.4	Maßregelungsprozess	☑		x	
6.5	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	☑	x	x	
6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	☑	x		
6.7	Telearbeit	☑		x	x
6.8	Meldung von Informationssicherheitsereignissen	☑	x	x	
7	**Physische Maßnahmen**				
7.1	Physische Sicherheitsperimeter	☑	x		x
7.2	Physischer Zutritt	☑	x		x
7.3	Sichern von Büros, Räumen und Einrichtungen	☑		x	x
7.4	Physische Sicherheitsüberwachung	☑	x		x
7.5	Schutz vor physischen und umweltbedingten Bedrohungen	☑	x	x	x
7.6	Arbeiten in Sicherheitsbereichen	☑	x		x
7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren	☑			x
7.8	Platzierung und Schutz von Geräten und Betriebsmitteln	☑		x	x
7.9	Sicherheit von Werten außerhalb der Räumlichkeiten	☑	x	x	x
7.10	Speichermedien	☑			x
7.11	Versorgungseinrichtungen	☑	x	x	x
7.12	Sicherheit der Verkabelung	☑		x	x
7.13	Instandhaltung von Geräten und Betriebsmitteln	☑		x	x
7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	☑			x

CompuGroup Medical Österreich
Statement of Applicability (SoA)
Version 3.0 (Public)

Maßnahmen ID (Control ID)	Maßnahmenbezeichnung (Control Name)	Anwendbar (gem. 6.1.3 d)	* Gründe für die Auswahl von Maßnahmenzielen und Maßnahmen (gem. 6.1.3 d)		
			CA	BO	RA
8	**Technologische Maßnahmen**				
8.1	Endpunktgeräte des Benutzers	☑	x		x
8.2	Privilegierte Zugangsrechte	☑			x
8.3	Informationszugangsbeschränkung	☑	x		x
8.4	Zugriff auf den Quellcode	☑		x	x
8.5	Sichere Authentifizierung	☑	x		x
8.6	Kapazitätssteuerung	☑		x	x
8.7	Schutz gegen Schadsoftware	☑	x	x	x
8.8	Handhabung von technischen Schwachstellen	☑		x	x
8.9	Konfigurationsmanagement	☑	x	x	x
8.10	Löschung von Informationen	☑	x	x	
8.11	Datenmaskierung	☑	x	x	
8.12	Verhinderung von Datenlecks	☑	x	x	x
8.13	Sicherung von Information	☑		x	x
8.14	Redundanz von informationsverarbeitenden Einrichtungen	☑	x	x	x
8.15	Protokollierung	☑	x		x
8.16	Überwachungstätigkeiten	☑	x		x
8.17	Uhrensynchronisation	☑			x
8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	☑			x
8.19	Installation von Software auf Systemen im Betrieb	☑	x	x	x
8.20	Netzwerksicherheit	☑	x	x	x
8.21	Sicherheit von Netzwerkdiensten	☑	x	x	x
8.22	Trennung von Netzwerken	☑	x	x	x
8.23	Webfilterung	☑		x	x
8.24	Verwendung von Kryptographie	☑	x	x	x
8.25	Lebenszyklus einer sicheren Entwicklung	☑		x	x
8.26	Anforderungen an die Anwendungssicherheit	☑	x	x	x

CompuGroup Medical Österreich
Statement of Applicability (SoA)
Version 3.0 (Public)

Maßnahmen ID (Control ID)	*Maßnahmenbezeichnung (Control Name)*	*Anwendbar (gem. 6.1.3 d)*	** Gründe für die Auswahl von Maßnahmenzielen und Maßnahmen (gem. 6.1.3 d)*		
			CA	*BO*	*RA*
8.27	Sichere Systemarchitektur und technische Grundsätze	☑		x	x
8.28	Sicheres Coding	☑		x	x
8.29	Sicherheitsprüfung bei Entwicklung und Abnahme	☑		x	x
8.30	Ausgegliederte Entwicklung	☑	x		x
8.31	Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen	☑		x	x
8.32	Änderungssteuerung	☑		x	x
8.33	Prüfinformationen	☑	x		x
8.34	Schutz der Informationssysteme während der Überwachungsprüfung	☑		x	x

* Legende für anwendbare Controls und Gründe für die Auswahl bestimmter Controls:

- **CA: Compliance Anfoderung (gesetzlich, vertraglich, regulatorisch)**
- **BO: Bussiness objective - Geschäftsanforderung bzw. -ziel**
- **RA: Risk Assessment - Ergebnis der Risikoeinschätzung**