Statement of Applicabilty - Inseya AG

Version: 1.0
29.05.2026

Bereich	Kapitel / Control aus Anhang A	Titel	Anwendbar?	Massnahme	Dokument (RL/VA, Prozess usw.), Veweis und Nachweis	Begründung der Anwendbarkeit	Umsetzungs-grad
	A.5.1	Informationssicherheitsrichtlinien	ja	Informationssicherheitsrichtlinien wurden definiert, kommuniziert und regelmässig überprüft.	ISMS Leitlinie	Erforderlich zur Steuerung des ISMS und zur Erfüllung interner Governance-Anforderungen.	Umgesetzt
	A.5.2	Informationssicherheitsrollen und -verantwortlichkeiten	ja	Rollen und Verantwortlichkeiten im Bereich Informationssicherheit sind definiert und organisatorisch verankert.	Organisationsrichtlinie Dokumentierte Prozesse	Rollen und Verantwortlichkeiten sind für die wirksame Umsetzung des ISMS notwendig.	Umgesetzt
	A.5.3	Aufgabentrennung	ja	Kritische Tätigkeiten und Berechtigungen werden organisatorisch getrennt und kontrolliert.	Rollenmodell Etablierte Prozesse, Richtlinie	Reduziert das Risiko von Fehlbedienung und Missbrauch bei kritischen Prozessen.	Umgesetzt
	A.5.4	Verantwortlichkeiten der Leitung	ja	Die Leitung unterstützt das ISMS durch definierte Verantwortlichkeiten, Steuerungsprozesse und regelmässige Bewertungen.	Sicherheitsrichtlinie Management Reviews	Managementverantwortung ist für wirksame ISMS-Steuerung erforderlich.	Umgesetzt
	A.5.5	Kontakt mit Behörden	ja	Prozesse zur Kommunikation mit relevanten Behörden und regulatorischen Stellen sind definiert.	Eskalationsprozess Dokumentierte Kommunikationsprozesse	Erforderlich zur Einhaltung gesetzlicher Melde- und Kommunikationspflichten.	Umgesetzt
	A.5.6	Kontakt mit speziellen Interessensgruppen	ja	Der Austausch mit relevanten Fachgruppen und Informationssicherheitsnetzwerken ist organisatorisch geregelt.	Dokumentierte Kommunikationsprozesse mit relevanten externen Stellen sowie definierte Eskalations- und Meldewege im ISMS	Erforderlich zur strukturierten Zusammenarbeit mit sicherheitsrelevanten externen Stellen und zur Unterstützung von Informationsaustausch im Sicherheitskontext.	Umgesetzt

	A.5.7	Bedrohungsintelligenz	ja	Relevante Informationen zu Bedrohungen und Schwachstellen werden beobachtet und bewertet.	Etablierte Prozesse zur Erfassung, Bewertung und Verarbeitung von Bedrohungsinformationen (z. B. Security Advisories, interne Bewertungen)	Unterstützt die proaktive Identifikation und Bewertung von Bedrohungen zur Reduzierung aktueller und zukünftiger Sicherheitsrisiken.	Umgesetzt
	A.5.8	Informationssicherheit im Projektmanagement	ja	Informationssicherheitsanforderungen werden in Projekten berücksichtigt und integriert.	Projektmanagement-Richtlinie mit integrierten Informationssicherheitsanforderungen und definierten Sicherheitsprüfpunkten	Erforderlich, um Informationssicherheitsanforderungen frühzeitig und systematisch in Projektvorhaben zu integrieren.	Umgesetzt
	A.5.9	Inventar der Informationen und anderen damit verbundenen Werten	ja	Informationswerte und relevante Assets werden identifiziert und verwaltet.	Asset-Management-Prozess inkl. Inventarisierung von Informationswerten und Zuordnung zu Schutzbedarfskategorien	Grundlage für den Schutz von Informationswerten durch vollständige Transparenz über relevante Assets und deren Bedeutung.	Umgesetzt
	A.5.10	Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten	ja	Anforderungen zur zulässigen Nutzung von Informationswerten sind definiert und kommuniziert.	Nutzungsrichtlinie für Informationswerte inkl. Acceptable Use Policy und verbindlichen organisatorischen Vorgaben	Sicherstellung eines regelkonformen und kontrollierten Umgangs mit Informationswerten innerhalb der Organisation.	Umgesetzt
	A.5.11	Rückgabe von Werten	ja	Prozesse zur Rückgabe von Informationswerten bei Austritt oder Rollenwechsel sind definiert.	Offboarding- und Übergabeprozess mit dokumentierter Rückgabe bzw. Sperrung von Informationswerten und Zugängen	Verhindert unkontrollierten Verbleib von Informationswerten bei Rollenwechseln oder Austritt von Mitarbeitenden.	Umgesetzt
	A.5.12	Klassifizierung von Information	ja	Informationen werden gemäss definierter Schutzbedarfe klassifiziert.	Klassifizierungsrichtlinie für Informationen inkl. definierter Schutzbedarfsstufen und Handhabungsvorgaben	Ermöglicht eine risikoorientierte Behandlung von Informationen entsprechend ihres Schutzbedarfs.	Umgesetzt

A.5 Organisatorische Massnahmen	A.5.13	Kennzeichnung von Information	ja	Anforderungen zur Kennzeichnung klassifizierter Informationen sind definiert.	Kennzeichnungsrichtlinie für Informationen inkl. Anforderungen an digitale und physische Markierung	Unterstützt die eindeutige Erkennbarkeit von Schutzanforderungen und reduziert Fehlbehandlung von Informationen.	Umgesetzt
	A.5.14	Informationsübertragung	ja	Anforderungen zur sicheren Übertragung von Informationen sind definiert und umgesetzt.	Richtlinie zur sicheren Informationsübertragung inkl. Vorgaben für verschlüsselte Kommunikation und sichere Kanäle	Reduziert Risiken bei der Übertragung sensibler Informationen durch definierte Schutzmechanismen.	Umgesetzt
	A.5.15	Zugangssteuerung	ja	Zugriffsrechte werden gemäss definierten Anforderungen verwaltet und regelmässig überprüft.	Zugriffskontrollrichtlinie inkl. Role-Based-Access-Ansatz und definierten Genehmigungsprozessen	Gewährleistet, dass nur berechtigte Personen Zugriff auf Informationen und Systeme erhalten.	Umgesetzt
	A.5.16	Identitätsmanagement	ja	Prozesse zur Verwaltung digitaler Identitäten und Zugriffsberechtigungen sind definiert.	Identity & Access Management Prozess inkl. Lifecycle von Benutzerkonten und Identitäten	Unterstützt die eindeutige Identifikation von Nutzern und die sichere Verwaltung digitaler Identitäten.	Umgesetzt
	A.5.17	Informationen zur Authentifizierung	ja	Anforderungen zur sicheren Verwaltung von Authentifizierungsinformationen sind definiert.	Passwort- und Authentifizierungsrichtlinie inkl. Anforderungen an sichere Anmeldeverfahren	Minimiert das Risiko von unautorisierten Zugriffen durch den Schutz von Authentifizierungsinformationen.	Umgesetzt
	A.5.18	Zugangsrechte	ja	Vergabe, Änderung und Entzug von Zugriffsrechten erfolgen kontrolliert und nachvollziehbar.	Berechtigungsmanagement-Prozess inkl. regelmässiger Rezertifizierung von Zugriffsrechten	Stellt sicher, dass Zugriffsrechte angemessen vergeben, überprüft und entzogen werden.	Umgesetzt
	A.5.19	Informationssicherheit in Lieferantenbeziehungen	ja	Sicherheitsanforderungen an Lieferanten und Dienstleister sind definiert.	Lieferantenmanagement-Richtlinie inkl. Sicherheitsanforderungen an externe Dienstleister	Reduziert Risiken aus Abhängigkeiten zu externen Dienstleistern und Lieferanten.	Umgesetzt
	A.5.20	Behandlung von Informationssicherheit in Lieferantenvereinbarungen	ja	Sicherheitsanforderungen werden vertraglich geregelt und überprüft.	Vertragsmanagement mit integrierten Informationssicherheitsklauseln für Lieferanten	Stellt sicher, dass Sicherheitsanforderungen verbindlich in Lieferantenbeziehungen verankert sind.	Umgesetzt

	A.5.21	Umgang mit der Informationssicherheit in der IKT-Lieferkette	ja	Risiken innerhalb der Lieferkette werden bewertet und gesteuert.	Risikomanagementprozess für die IKT-Lieferkette inkl. Bewertung kritischer Dienstleister	Unterstützt die durchgängige Steuerung von Informationssicherheitsrisiken entlang der Lieferkette.	Umgesetzt
	A.5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	ja	Lieferantendienstleistungen werden regelmässig bewertet und überwacht.	Lieferanten-Performance- und Sicherheitsbewertungsprozess inkl. regelmässiger Reviews	Gewährleistet, dass externe Dienstleistungen kontinuierlich auf Sicherheitsanforderungen überprüft werden.	Umgesetzt
	A.5.23	Informationssicherheit für die Nutzung von Cloud-Diensten	ja	Sicherheitsanforderungen für Cloud-Dienste sind definiert und werden bewertet.	Cloud-Governance-Richtlinie inkl. Sicherheits- und Risikobewertung von Cloud Services	Minimiert Risiken bei der Nutzung von Cloud-Diensten durch definierte Sicherheitsanforderungen.	Umgesetzt
	A.5.24	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	ja	Prozesse zum Umgang mit Informationssicherheitsvorfällen sind definiert.	Incident-Management-Prozess inkl. Meldewege und Reaktionsstrukturen	Ermöglicht eine strukturierte und schnelle Vorbereitung auf sicherheitsrelevante Ereignisse.	Umgesetzt
	A.5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse	ja	Sicherheitsvorfälle werden bewertet und gemäss definierten Kriterien behandelt.	Klassifizierungs- und Bewertungsschema für Sicherheitsvorfälle	Stellt sicher, dass Vorfälle konsistent bewertet und angemessen klassifiziert werden.	Umgesetzt
	A.5.26	Reaktion auf Informationssicherheitsvorfälle	ja	Massnahmen zur Reaktion auf Sicherheitsvorfälle sind definiert und etabliert.	Incident Response Playbooks und definierte Reaktionsprozesse	Unterstützt eine wirksame Eindämmung und Behandlung von Sicherheitsvorfällen.	Umgesetzt
	A.5.27	Erkenntnisse aus Informationssicherheitsvorfällen	ja	Sicherheitsvorfälle werden analysiert und Verbesserungsmassnahmen abgeleitet.	Post-Incident-Review Prozess inkl. Lessons-Learned Dokumentation	Fördert die kontinuierliche Verbesserung der Informationssicherheit durch systematische Analyse von Vorfällen.	Umgesetzt
	A.5.28	Sammeln von Beweismaterial	ja	Anforderungen zur Sicherung relevanter Nachweise bei Sicherheitsvorfällen sind definiert.	Forensische Sicherungsrichtlinie inkl. Aufbewahrung und Schutz von Beweismitteln	Unterstützt rechtliche und forensische Anforderungen durch die gesicherte Behandlung von Beweismitteln.	Umgesetzt

	A.5.29	Informationssicherheit bei Störungen	ja	Prozesse zur Aufrechterhaltung der Informationssicherheit bei Störungen sind definiert.	Business Continuity und IT-Service-Continuity Verfahren	Stellt sicher, dass Informationssicherheit auch bei betrieblichen Störungen aufrechterhalten wird.	Umgesetzt
	A.5.30	IKT-Bereitschaft für Business Continuity	ja	Anforderungen zur Wiederherstellung und Verfügbarkeit kritischer Systeme sind definiert.	Wiederherstellungs- und Disaster-Recovery-Prozess für kritische Systeme	Unterstützt die Wiederherstellung geschäftskritischer Funktionen im Rahmen der Geschäftskontinuität.	Umgesetzt
	A.5.31	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen	ja	Relevante gesetzliche und vertragliche Anforderungen werden identifiziert und berücksichtigt.	Compliance Management Prozess zur Identifikation regulatorischer Anforderungen	Gewährleistet die systematische Einhaltung gesetzlicher, regulatorischer und vertraglicher Anforderungen.	Umgesetzt
	A.5.32	Geistige Eigentumsrechte	ja	Anforderungen zum Schutz geistigen Eigentums sind definiert.	Intellectual Property Schutzrichtlinie und vertragliche Schutzmechanismen	Schützt geistige Eigentumsrechte und verhindert unbefugte Nutzung oder Offenlegung.	Umgesetzt
	A.5.33	Schutz von Aufzeichnungen	ja	Anforderungen zur Aufbewahrung und zum Schutz relevanter Aufzeichnungen sind definiert.	Records Management und Archivierungsrichtlinie	Unterstützt Nachvollziehbarkeit, rechtliche Anforderungen und revisionssichere Aufbewahrung von Informationen.	Umgesetzt
	A.5.34	Datenschutz und Schutz personenbezogener Daten (pbD)	ja	Datenschutzanforderungen werden organisatorisch und technisch umgesetzt.	Datenschutzmanagementsystem (DSMS) bzw. Datenschutzrichtlinie	Stellt die Einhaltung von Datenschutz- und Privatsphärenanforderungen sicher.	Umgesetzt
	A.5.35	Unabhängige Überprüfung der Informationssicherheit	ja	Informationssicherheitsmassnahmen werden regelmässig unabhängig überprüft.	Internes Auditprogramm und unabhängige ISMS-Reviews	Ermöglicht eine unabhängige Bewertung der Wirksamkeit des ISMS.	Umgesetzt
	A.5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	ja	Die Einhaltung definierter Sicherheitsvorgaben wird regelmässig überprüft.	Compliance Monitoring Prozess inkl. regelmässiger Kontrollprüfungen	Unterstützt die kontinuierliche Einhaltung definierter Sicherheitsrichtlinien und Standards.	Umgesetzt

	A.5.37	Dokumentierte Betriebsabläufe	ja	Relevante Betriebsverfahren werden dokumentiert und gepflegt.	Dokumentations- und Prozessmanagement-Richtlinie für Betriebsverfahren	Sichert konsistente und nachvollziehbare Betriebsabläufe durch dokumentierte Verfahren.	Umgesetzt
A.6 Personenbezogene Massnahmen	A.6.1	Sicherheitsüberprüfung	ja	Sicherheitsrelevante Prüfungen vor Beschäftigungsbeginn sind definiert.	Interne Richtlinien, Prozesse und Nachweise	Reduziert personelle Sicherheitsrisiken bereits vor Beginn eines Beschäftigungsverhältnisses.	Umgesetzt
	A.6.2	Beschäftigungs- und Vertragsbedingungen	ja	Informationssicherheitsanforderungen sind Bestandteil der Beschäftigungsbedingungen.	Interne Richtlinien, Prozesse und Nachweise	Verankert Informationssicherheitsanforderungen verbindlich in Beschäftigungsverhältnissen.	Umgesetzt
	A.6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung	ja	Mitarbeitende werden regelmässig zu Informationssicherheit sensibilisiert und geschult.	Interne Richtlinien, Prozesse und Nachweise	Stärkt das Sicherheitsbewusstsein und reduziert menschliche Fehler als Risikofaktor.	Umgesetzt
	A.6.4	Massregelungsprozess	ja	Prozesse für den Umgang mit Verstössen gegen Sicherheitsanforderungen sind definiert.	Interne Richtlinien, Prozesse und Nachweise	Unterstützt die konsequente Durchsetzung von Sicherheitsvorgaben innerhalb der Organisation.	Umgesetzt
	A.6.5	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	ja	Sicherheitsrelevante Anforderungen bei Austritt oder Rollenwechsel sind definiert.	Interne Richtlinien, Prozesse und Nachweise	Stellt sicher, dass Zugriffsrechte und Verantwortlichkeiten bei Veränderungen korrekt angepasst werden.	Umgesetzt
	A.6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	ja	Vertraulichkeitsanforderungen werden vertraglich geregelt.	Interne Richtlinien, Prozesse und Nachweise	Schützt vertrauliche Informationen durch vertraglich geregelte Geheimhaltungspflichten.	Umgesetzt
	A.6.7	Telearbeit	ja	Sicherheitsanforderungen für mobiles Arbeiten sind definiert und umgesetzt.	Interne Richtlinien, Prozesse und Nachweise	Reduziert Risiken beim Arbeiten ausserhalb gesicherter Unternehmensumgebungen.	Umgesetzt

	A.6.8	Meldung von Informationssicherheitsereignissen	ja	Prozesse zur Meldung sicherheitsrelevanter Ereignisse sind etabliert.	Interne Richtlinien, Prozesse und Nachweise	Unterstützt die frühzeitige Erkennung und Behandlung sicherheitsrelevanter Ereignisse.	Umgesetzt
A.7 Physische Massnahmen	A.7.1	Physische Sicherheitsperimeter	ja	Physische Sicherheitsbereiche werden geschützt und kontrolliert.	Interne Richtlinien, Prozesse und Nachweise	Schützt physische Bereiche vor unautorisiertem Zugriff und Umweltrisiken.	Umgesetzt
	A.7.2	Physischer Zutritt	ja	Zutrittsrechte zu sensiblen Bereichen werden kontrolliert verwaltet.	Interne Richtlinien, Prozesse und Nachweise	Stellt kontrollierten Zugang zu sicherheitskritischen Bereichen sicher.	Umgesetzt
	A.7.3	Sichern von Büros, Räumen und Einrichtungen	ja	Schutzmassnahmen für Arbeitsbereiche und Einrichtungen sind definiert.	Interne Richtlinien, Prozesse und Nachweise	Reduziert Risiken durch Schutz von Arbeits- und Betriebsumgebungen.	Umgesetzt
	A.7.4	Physische Sicherheitsüberwachung	ja	Sicherheitsrelevante Bereiche werden angemessen überwacht.	Interne Richtlinien, Prozesse und Nachweise	Unterstützt die Erkennung unautorisierter physischer Aktivitäten.	Umgesetzt
	A.7.5	Schutz vor physischen und umweltbedingten Bedrohungen	ja	Massnahmen zum Schutz vor physischen und umgebungsbedingten Risiken sind definiert.	Interne Richtlinien, Prozesse und Nachweise	Minimiert Risiken durch physische oder umgebungsbedingte Einflüsse.	Umgesetzt
	A.7.6	Arbeiten in Sicherheitsbereichen	ja	Sicherheitsanforderungen für Tätigkeiten in geschützten Bereichen sind definiert.	Interne Richtlinien, Prozesse und Nachweise	Stellt sicher, dass Tätigkeiten in Sicherheitsbereichen kontrolliert erfolgen.	Umgesetzt
	A.7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren	ja	Anforderungen zur sicheren Nutzung von Arbeitsplätzen sind definiert.	Interne Richtlinien, Prozesse und Nachweise	Reduziert das Risiko unbeabsichtigter Informationsoffenlegung am Arbeitsplatz.	Umgesetzt
	A.7.8	Platzierung und Schutz von Geräten und Betriebsmitteln	ja	Kritische Einrichtungen werden unter Berücksichtigung relevanter Risiken geschützt.	Interne Richtlinien, Prozesse und Nachweise	Unterstützt die resiliente Standortwahl kritischer Einrichtungen.	Umgesetzt
	A.7.9	Sicherheit von Werten ausserhalb der Räumlichkeiten	ja	Informationswerte ausserhalb definierter Standorte werden angemessen geschützt.	Interne Richtlinien, Prozesse und Nachweise	Schützt Informationswerte ausserhalb kontrollierter Unternehmensumgebungen.	Umgesetzt

	A.7.10	Speichermedien	ja	Anforderungen zum sicheren Umgang mit Speichermedien sind definiert.	Interne Richtlinien, Prozesse und Nachweise	Verhindert Verlust oder unbefugte Nutzung von Daten auf Speichermedien.	Umgesetzt
	A.7.11	Versorgungseinrichtungen	ja	Kritische Versorgungseinrichtungen werden überwacht und geschützt.	Interne Richtlinien, Prozesse und Nachweise	Stellt die Verfügbarkeit kritischer Infrastruktur durch stabile Versorgung sicher.	Umgesetzt
	A.7.12	Sicherheit der Verkabelung	ja	Kommunikations- und Stromverkabelung werden geschützt und kontrolliert.	Interne Richtlinien, Prozesse und Nachweise	Schützt technische Infrastruktur vor Manipulation oder Ausfall.	Umgesetzt
	A.7.13	Instandhaltung von Geräten und Betriebsmitteln	ja	Geräte werden regelmässig gewartet und kontrolliert betrieben.	Interne Richtlinien, Prozesse und Nachweise	Unterstützt die zuverlässige und sichere Nutzung von Geräten.	Umgesetzt
	A.7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	ja	Prozesse zur sicheren Entsorgung und Wiederverwendung von Geräten sind definiert.	Interne Richtlinien, Prozesse und Nachweise	Verhindert Datenabfluss durch sichere Entsorgung oder Wiederverwendung von Geräten.	Umgesetzt
	A.8.1	Endpunktgeräte des Benutzers	ja	Sicherheitsanforderungen für Benutzerendgeräte sind definiert und umgesetzt.	Richtlinien, Betriebs- und Sicherheitsprozesse dokumentiert.	Unterstützt den Schutz von Informationen und Systemen auf Benutzerendgeräten.	Umgesetzt
	A.8.2	Privilegierte Zugangsrechte	ja	Vergabe und Nutzung privilegierter Zugriffsrechte werden kontrolliert und regelmässig überprüft.	Berechtigungs- und Kontrollprozesse dokumentiert.	Unterstützt den Schutz vor unautorisierten oder missbräuchlichen Aktivitäten.	Umgesetzt
	A.8.3	Informationszugangsbeschränkung	ja	Zugriffe auf Informationen und Systeme werden gemäss definierten Anforderungen beschränkt.	Zugriffskonzepte und Kontrollprozesse dokumentiert.	Unterstützt Vertraulichkeit und Integrität von Informationen.	Umgesetzt
	A.8.4	Zugriff auf den Quellcode	ja	Der Zugriff auf Quellcode wird kontrolliert und auf autorisierte Personen beschränkt.	Entwicklungs- und Berechtigungsprozesse dokumentiert.	Unterstützt den Schutz vor unautorisierten Änderungen und Offenlegung.	Umgesetzt
	A.8.5	Sichere Authentifizierung	ja	Anforderungen an sichere Authentifizierungsverfahren sind definiert und umgesetzt.	Sicherheitsrichtlinien und Betriebsprozesse dokumentiert.	Unterstützt den Schutz vor unautorisiertem Zugriff.	Umgesetzt

A.8.6	Kapazitätssteuerung	ja	Kapazitäten kritischer Systeme werden überwacht und geplant.	Monitoring- und Betriebsprozesse dokumentiert.	Unterstützt die Verfügbarkeit und Leistungsfähigkeit geschäftskritischer Systeme.	Umgesetzt
A.8.7	Schutz gegen Schadsoftware	ja	Massnahmen zum Schutz vor Schadsoftware sind definiert und etabliert.	Sicherheits- und Monitoringprozesse dokumentiert.	Unterstützt den Schutz vor Schadsoftware und sicherheitsrelevanten Bedrohungen.	Umgesetzt
A.8.8	Handhabung von technischen Schwachstellen	ja	Technische Schwachstellen werden identifiziert, bewertet und behandelt.	Schwachstellenmanagement- und Patchprozesse dokumentiert.	Unterstützt die Reduzierung technischer Sicherheitsrisiken.	Umgesetzt
A.8.9	Konfigurationsmanagement	ja	Sicherheitsrelevante Konfigurationen werden definiert und kontrolliert verwaltet.	Konfigurations- und Betriebsprozesse dokumentiert.	Unterstützt stabile und sichere Betriebsumgebungen.	Umgesetzt
A.8.10	Löschung von Informationen	ja	Anforderungen zur sicheren Löschung von Informationen sind definiert und umgesetzt.	Lösch- und Entsorgungsprozesse dokumentiert.	Unterstützt den Schutz vertraulicher Informationen während des gesamten Lebenszyklus.	Umgesetzt
A.8.11	Datenmaskierung	ja	Verfahren zur Maskierung sensibler Daten werden eingesetzt, sofern erforderlich.	Datenschutz- und Sicherheitsprozesse dokumentiert.	Unterstützt den Schutz sensibler und personenbezogener Informationen.	Umgesetzt
A.8.12	Verhinderung von Datenlecks	ja	Massnahmen zur Verhinderung und Erkennung von Datenverlusten sind definiert.	Sicherheits- und Monitoringprozesse dokumentiert.	Unterstützt den Schutz vertraulicher und geschäftskritischer Informationen.	Umgesetzt
A.8.13	Sicherung von Information	ja	Datensicherungen werden regelmässig erstellt, geschützt und überprüft.	Backup- und Wiederherstellungsprozesse dokumentiert.	Unterstützt die Wiederherstellbarkeit und Verfügbarkeit geschäftskritischer Informationen.	Umgesetzt
A.8.14	Redundanz von informationsverarbeitenden Einrichtungen	ja	Kritische Systeme und Dienste werden durch geeignete Redundanzmassnahmen abgesichert.	Infrastruktur- und Kontinuitätsprozesse dokumentiert.	Unterstützt die Verfügbarkeit kritischer Systeme und Dienstleistungen.	Umgesetzt

A.8 Technologische Massnahmen	A.8.15	Protokollierung	ja	Sicherheitsrelevante Ereignisse werden protokolliert und ausgewertet.	Logging- und Monitoringprozesse dokumentiert.	Unterstützt die Nachvollziehbarkeit und Erkennung sicherheitsrelevanter Aktivitäten.	Umgesetzt
	A.8.16	Überwachung von Aktivitäten	ja	Systeme und Sicherheitsereignisse werden kontinuierlich überwacht.	Monitoring- und Incident-Management-Prozesse dokumentiert.	Unterstützt die frühzeitige Erkennung sicherheitsrelevanter Ereignisse.	Umgesetzt
	A.8.17	Uhrensynchronisation	ja	Systeme verwenden konsistente und kontrollierte Zeitquellen.	Infrastruktur- und Betriebsprozesse dokumentiert.	Unterstützt die Integrität von Protokollen und sicherheitsrelevanten Ereignissen.	Umgesetzt
	A.8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	ja	Die Nutzung administrativer Hilfsprogramme wird kontrolliert und eingeschränkt.	Berechtigungs- und Kontrollprozesse dokumentiert.	Unterstützt den Schutz vor missbräuchlicher Nutzung administrativer Funktionen.	Umgesetzt
	A.8.19	Installation von Software auf Systemen im Betrieb	ja	Softwareinstallationen erfolgen kontrolliert und gemäss definierten Anforderungen.	Betriebs- und Freigabeprozesse dokumentiert.	Unterstützt stabile und sichere Systemumgebungen.	Umgesetzt
	A.8.20	Netzwerksicherheit	ja	Sicherheitsmassnahmen zum Schutz von Netzwerken und Kommunikationsverbindungen sind definiert.	Netzwerk- und Sicherheitsprozesse dokumentiert.	Unterstützt Vertraulichkeit, Integrität und Verfügbarkeit der Kommunikation.	Umgesetzt
	A.8.21	Sicherheit von Netzwerkdiensten	ja	Sicherheitsanforderungen für Netzwerkdienste werden definiert und überwacht.	Betriebs- und Sicherheitsprozesse dokumentiert.	Unterstützt den sicheren Betrieb von Netzwerkdiensten.	Umgesetzt
	A.8.22	Trennung von Netzwerken	ja	Netzwerke und Systeme werden gemäss Sicherheitsanforderungen segmentiert.	Netzwerk- und Infrastrukturprozesse dokumentiert.	Unterstützt die Reduzierung von Sicherheitsrisiken und unautorisierten Zugriffen.	Umgesetzt
	A.8.23	Webfilterung	ja	Massnahmen zur Kontrolle und Filterung von Webzugriffen sind definiert.	Sicherheits- und Nutzungsrichtlinien dokumentiert.	Unterstützt den Schutz vor schädlichen oder unangemessenen Inhalten.	Umgesetzt
	A.8.24	Verwendung von Kryptographie	ja	Kryptographische Verfahren werden gemäss definierten Anforderungen eingesetzt.	Kryptographie- und Sicherheitsrichtlinien dokumentiert.	Unterstützt den Schutz vertraulicher Informationen und Kommunikationswege.	Umgesetzt

	A.8.25	Lebenszyklus einer sicheren Entwicklung	ja	Sicherheitsanforderungen werden im Entwicklungsprozess berücksichtigt.	Entwicklungs- und Sicherheitsprozesse dokumentiert.	Unterstützt die Entwicklung sicherer Anwendungen und Systeme.	Umgesetzt
	A.8.26	Anforderungen an die Anwendungssicherheit	ja	Sicherheitsanforderungen für Anwendungen werden definiert und überprüft.	Entwicklungs- und Governance-Prozesse dokumentiert.	Unterstützt die sichere Entwicklung und den sicheren Betrieb von Anwendungen.	Umgesetzt
	A.8.27	Sichere Systemarchitektur und technische Grundsätze	ja	Sicherheitsanforderungen werden bei Architektur und Entwicklung berücksichtigt.	Architektur- und Entwicklungsprozesse dokumentiert.	Unterstützt die Sicherheit von Systemen und Anwendungen über deren Lebenszyklus.	Umgesetzt
	A.8.28	Sicheres Coding	ja	Anforderungen an sicheres Programmieren sind definiert und werden berücksichtigt.	Entwicklungsrichtlinien und Qualitätsprozesse dokumentiert.	Unterstützt die Reduzierung softwarebezogener Sicherheitsrisiken.	Umgesetzt
	A.8.29	Sicherheitsprüfung in Entwicklung und Abnahme	ja	Sicherheitsprüfungen werden im Entwicklungs- und Freigabeprozess durchgeführt.	Test- und Freigabeprozesse dokumentiert.	Unterstützt die Identifikation sicherheitsrelevanter Schwachstellen vor Produktivsetzung.	Umgesetzt
	A.8.30	Ausgegliederte Entwicklung	ja	Sicherheitsanforderungen an externe Entwicklungsdienstleistungen sind definiert.	Lieferanten- und Entwicklungsprozesse dokumentiert.	Unterstützt die Steuerung von Risiken bei ausgelagerter Entwicklung.	Umgesetzt
	A.8.31	Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen	ja	Entwicklungs-, Test- und Produktivumgebungen werden getrennt betrieben.	Infrastruktur- und Betriebsprozesse dokumentiert.	Unterstützt die Reduzierung von Risiken durch unkontrollierte Änderungen oder Zugriffe.	Umgesetzt
	A.8.32	Änderungssteuerung	ja	Änderungen an Systemen und Anwendungen erfolgen kontrolliert und nachvollziehbar.	Change-Management- und Freigabeprozesse dokumentiert.	Unterstützt stabile und sichere Betriebsumgebungen.	Umgesetzt
	A.8.33	Prüfinformationen	ja	Der Umgang mit Testinformationen erfolgt gemäss definierten Sicherheitsanforderungen.	Entwicklungs- und Datenschutzprozesse dokumentiert.	Unterstützt den Schutz sensibler Informationen in Testumgebungen.	Umgesetzt
	A.8.34	Schutz der Informationssysteme während der Überwachungsprüfung	ja	Sicherheitsmassnahmen während Audit- und Prüfaktivitäten sind definiert.	Audit- und Sicherheitsprozesse dokumentiert.	Unterstützt die Integrität und Verfügbarkeit produktiver Systeme während Prüfungen.	Umgesetzt