A-Trust GmbH
1030 Wien, Landstraßer Hauptstraße 1b, E02

1 Statement of Applicability (SoA) ISO27002:2022

Nummer	Kontrolle	Anwendbar	Umgesetzt
A5.1	Richtlinien für die Informationssicherheit	Ja	Ja
A5.2	Rollen und Verantwortlichkeiten	Ja	Ja
A5.3	Trennung der Aufgaben	Ja	Ja
A5.4	Verantwortlichkeiten Management	Ja	Ja
A5.5	Kontakt mit Behörden	Ja	Ja
A5.6	Kontakt mit Interessengruppen	Ja	Ja
A5.7	Informationen über Bedrohungen	Ja	Ja
A5.8	Informationssicherheit im Projektmanagement	Ja	Ja
A5.9	Inventar der Informationen und anderer zugehöriger Vermögenswerte	Ja	Ja
A5.10	Zulässige Nutzung von Vermögenswerten und anderen zugehörigen Informationswerten	Ja	Ja
A5.11	Return of assets	Ja	Ja
A5.12	Klassifizierung von Informationen	Ja	Ja
A5.13	Kennzeichnung von Informationen	Ja	Ja
A5.14	Informationstransfer	Ja	Ja
A5.15	Zugangskontrolle	Ja	Ja
A5.16	Identitätsverwaltung	Ja	Ja
A5.17	Authentication of information	Ja	Ja
A5.18	Zugangsberechtigungen	Ja	Ja
A5.19	Informationssicherheit der Zulieferer	Ja	Ja
A5.20	Berücksichtigung der Sicherheit in Lieferentenvereinbarungen	Ja	Ja
A5.21	Management der Informationssicherheit in der IKT-Lieferkette	Ja	Ja
A5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantenleistungen	Ja	Ja

A5.23	Information security for use of cloud services	Ja	Ja
A5.24	Management von Informationssicherheitsvorfällen - Planung und Vorbereitung	Ja	Ja
A5.25	Management von Informationssicherheitsvorfällen - Bewertung und Entscheidung über Ereignisse im Bereich der Informationssicherheit	Ja	Ja
A5.26	Management von Informationssicherheitsvorfällen - Reaktion auf Vorfälle im Bereich der Informationssicherheit	Ja	Ja
A5.27	Management von Informationssicherheitsvorfällen - Aus Vorfällen im Bereich der Informationssicherheit lernen	Ja	Ja
A5.28	Management von Informationssicherheitsvorfällen - Sammlung von Beweisen	Ja	Ja
A5.29	Management von Informationssicherheitsvorfällen - Informationssicherheit während der Unterbrechung	Ja	Ja
A5.30	IKT Einsatzbereitschaft zur Betriebskontinuität	Ja	Ja
A5.31	Identifizierung der geltenden gesetzlichen und vertraglichen Anforderungen	Ja	Ja
A5.32	Rechte an geistigem Eigentum	Ja	Ja
A5.33	Schutz von Unterlagen	Ja	Ja
A5.34	Privatsphäre und Persönliche Informationen zur Identifizierung	Ja	Ja
A5.35	Unabhängige Überprüfung der Informationssicherheit	Ja	Ja
A5.36	Einhaltung von Strategien, Regeln und Standards für die Informationssicherheit	Ja	Ja
A5.37	Dokumentierte Betriebsverfahren	Ja	Ja
A6.1	Überprüfung	Ja	Ja
A6.2	Arbeitsvertrag und Arbeitsbedingungen	Ja	Ja
A6.3	Bewusstsein für Informationssicherheit, Aufklärung und Schulung	Ja	Ja
A6.4	Disziplinarverfahren	Ja	Ja
A6.5	Verantwortlichkeiten nach Beendigung oder Wechsel des Beschäftigungsverhältnisses	Ja	Ja
A6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	Ja	Ja

A6.7	Telearbeit	Ja	Ja
A6.8	Berichterstattung über Ereignisse im Bereich der Informationssicherheit	Ja	Ja
A7.1	Physischer Sicherheitsperimeter	Ja	Ja
A7.2	Physische Zugangskontrollen	Ja	Ja
A7.3	Sicherung von Büros, Räumen und Einrichtungen	Ja	Ja
A7.4	Physische Sicherheitsüberwachung	Ja	Ja
A7.5	Schutz vor physischen und Umweltbedrohungen	Ja	Ja
A7.6	Arbeiten in Sicherheitsbereichen	Ja	Ja
A7.7	Politik des freien Schreibtisches und des leeren Bildschirms (Clear desk, clear screen policy)	Ja	Ja
A7.8	Geräte-Standortwahl und Schutz	Ja	Ja
A7.9	Sicherheit von Vermögenswerten außerhalb von Geschäftsräumen	Ja	Ja
A7.10	Speichermedien	Ja	Ja
A7.11	Unterstützende Versorgungseinrichtungen	Ja	Ja
A7.12	Sicherheit der Verkabelung	Ja	Ja
A7.13	Wartung der Geräte	Ja	Ja
A7.14	Sichere Entsorgung oder Wiederverwendung von Geräten	Ja	Ja
A8.1	Endgeräte für Benutzer	Ja	Ja
A8.2	Privilegierte Zugangsberechtigung	Ja	Ja
A8.3	Beschränkung des Zugangs zu Informationen	Ja	Ja
A8.4	Zugriff auf den Quellcode	Ja	Ja
A8.5	Gesicherte Authentifizierung	Ja	Ja
A8.6	Kapazitätsmanagement	Ja	Ja
A8.7	Schutz vor Malware	Ja	Ja
A8.8	Verwaltung technischer Schwachstellen	Ja	Ja
A8.9	Konfigurationsmanagement	Ja	Ja
A8.10	Löschung von Informationen	Ja	Ja
A8.11	Daten Maskierung (Verschleierung)	Ja	Ja

A8.12	Verhinderung von Daten-Lecks (unberechtigter Datenabfluss)	Ja	Ja
A8.13	Backup Konzept	Ja	Ja
A8.14	Redundanzen bei Informationsverarbeitungs-Anlagen	Ja	Ja
A8.15	Logging	Ja	Ja
A8.16	Monitoring Aktivitäten	Ja	Ja
A8.17	Synchronisierung der Urzeit	Ja	Ja
A8.18	Nutzung von Software die priviligierte Rechte benötigt	Ja	Ja
A8.19	Installation von Software auf operationellen Systemen	Ja	Ja
A8.20	Sicherheit im Netzwerk	Ja	Ja
A8.21	Sicherheit der Netzwerkdienste	Ja	Ja
A8.22	Segregation in Netzen	Ja	Ja
A8.23	Web-Filterung	Ja	Ja
A8.24	Nutzung von Kryptographischen Maßnahmen	Ja	Ja
A8.25	Sicherer Lebenszyklus für die Softwareentwicklung	Ja	Ja
A8.26	Sicherheitsanforderungen für Anwendungen	Ja	Ja
A8.27	Sichere Systemarchitektur und technische Grundsätze	Ja	Ja
A8.28	Sichere Programmierung	Ja	Ja
A8.29	Sicherheitstests bei Entwicklung und Abnahme	Ja	Ja
A8.30	Ausgelagerte Entwicklung	Ja	Ja
A8.31	Trennung von Entwicklungs- (testing), Test- (staging), und Produktiv-Systemen (production)	Ja	Ja
A8.32	Veränderungsmanagement	Ja	Ja
A8.33	Test Information	Ja	Ja
A8.34	Schutz der Informationssysteme während des Audits	Ja	Ja