A1 Mindest-Sicherheitsstandard für Lieferanten

Version 1.1

Standard für das
A1 Informationssicherheitsmanagement

A1 Mindest-Sicherheitsstandard für Lieferanten – v1.1
A1 OneSEC
Gültig ab 15.09.2024
Klassifizierung: Öffentlich | TLP: CLEAR

Inhalt

1. Geltungsbereich & generelle Zielsetzung

Im digitalen Zeitalter ist die Sicherheit von Informationen von entscheidender Bedeutung, insbesondere für Telekommunikationsunternehmen, die täglich mit sensiblen Daten operieren. Dieses Dokument legt die Mindest-Sicherheitsanforderungen für Lieferanten (nachstehend auch: Auftragnehmer, externe Partner, Supplier, Provider, 3rd Party, Dienstleister oder Auftragsverarbeiter genannt) von A1 fest. Lieferanten sind damit alle externen Unternehmen, Organisationen oder Einzelpersonen, die Waren oder Dienstleistungen an die A1 liefern. Dies umfasst sowohl physische Güter als auch (digitale) Dienstleistungen und Softwarelösungen. Auch dazu gehören strategische Partner, Berater und andere Drittparteien, die Zugang zu Informationssystemen oder Daten von A1 haben.

Die genannten Anforderungen müssen vom Lieferanten rechtlich bindend mit seinen Lieferanten (nachstehend „4th Parties", Sub-Lieferanten, Lieferanten des Lieferanten) vereinbart werden. Diese Vereinbarungen dürfen keine geringeren Anforderungen enthalten als in diesem Standard festgelegt.

Ziel ist es, die Integrität, Vertraulichkeit und Verfügbarkeit der Informationsressourcen von A1 zu gewährleisten.

Um die Einhaltung dieser Anforderungen zu erleichtern, enthält dieses Dokument in Anhang A ein detailliertes Mapping jeder Kontrolle auf die Norm ISO 27001:2022. Lieferanten, die bereits über eine ISO 27001-Zertifizierung verfügen, können dadurch leicht erkennen, welche der geforderten Kontrollen sie aller Voraussicht nach bereits durch ihre bestehende Zertifizierung erfüllen. Diese Kontrollen sind auch in den jeweiligen Kapiteln mit einem ISO27001 Symbol versehen. Dies reduziert den Aufwand für die Implementierung zusätzlicher Sicherheitsmaßnahmen und fördert eine standardisierte Sicherheitskultur zwischen den involvierten Unternehmen.

A1 erwartet von allen Lieferanten, dass sie diese Sicherheitsanforderungen vollständig erfüllen und damit zur Sicherheit der gemeinsamen Geschäftsbeziehungen beitragen.

2. Lieferanten-Risikomanagement der A1

Das Lieferanten-Risikomanagement der A1 stellt sicher, dass alle Lieferanten - insbesondere jene, die A1 als besonders sicherheitsrelevant einstuft - den hohen Sicherheitsstandards des Telekommunikationsunternehmens sowie den regulatorischen Anforderungen (z.B. Netz- und Informationssicherheitsgesetz – NISG, Telekommunikations-Netzsicherheitsverordnung – TK-NSiV) entsprechen. Im Folgenden werden die wichtigsten Aspekte und Erwartungen, die A1 an Lieferanten hat, erläutert:

Einhaltung der Sicherheitsvorgaben

Lieferanten sind verpflichtet, die A1 Sicherheitsvorgaben für Lieferanten sorgfältig zu prüfen und zu gewährleisten, dass sie diese erfüllen können. Dies umfasst alle in diesem Dokument festgelegten Mindest-Sicherheitsanforderungen.

Mitteilung von Abweichungen
Sollten Lieferanten feststellen, dass sie einzelne Sicherheitsvorgaben nicht einhalten können, müssen sie dies A1 unverzüglich an die Mail-Adresse SupplyChainSecurity@a1.at mitteilen. In solchen Fällen wird A1 prüfen, ob die Kontrollabweichung ein Risiko für das Unternehmen darstellt.

Risikomitigation
Es ist notwendig, dass Lieferanten A1 informieren, ob und wodurch sie Risiken, die durch eine Kontrollabweichung entstehen (könnten), mitigieren. Dazu müssen Lieferanten detaillierte Informationen über die getroffenen oder geplanten Maßnahmen zur Risikominderung auf Nachfrage von A1 zur Verfügung stellen.

Regelmäßige Sicherheitsbewertungen bei Lieferanten mit hoher Sicherheitsrelevanz
A1 erwartet von allen Lieferanten, welche als besonders sicherheitsrelevant eingestuft werden (z.B., weil ihre Produkte und/oder Dienstleistungen zu Sarbanes-Oxley Act „SOX", Digital Operational Resilience Act „DORA" oder NISG-relevanten Diensten beitragen), dass sie innerhalb von 36 Monaten zumindest einmal für ein persönliches Gespräch zur Evaluierung ihres Sicherheitsstatus zur Verfügung stehen, und dafür auch personelle sowie zeitliche Kapazitäten durch die Lieferanten vorgesehen werden. Dieses Gespräch dient dazu, die aktuellen Sicherheitsmaßnahmen des Lieferanten zu bewerten und sicherzustellen, dass diese den Anforderungen von A1 entsprechen.

Durch diesen proaktiven Ansatz im Lieferanten-(Risiko-)management stellt A1 sicher, dass die Informationssicherheit auf höchstem Niveau bleibt und potenzielle Risiken frühzeitig identifiziert und adressiert werden können.

3. Definitionen

In mehreren der angeführten Vorgaben finden sich Elemente wie:

- **„CVSS"**: Das „Common Vulnerability Scoring System" (CVSS) ist ein freies und allgemeines System zur Bewertung des Schweregrades von Computersicherheitslücken. Es liefert eine numerische Bewertung, die hilft, die Dringlichkeit und das Risiko von Sicherheitslücken zu verstehen und priorisieren. Nähere Informationen zum CVSS finden Sie hier: CVSS v4.0 Specification Document (first.org).

- **„CIS-Benchmarks"**: Diese Benchmarks sind eine Reihe von Best-Practice-Richtlinien und Konfigurationsempfehlungen, die vom „Center for Internet Security" (CIS) entwickelt wurden. Sie bieten detaillierte, konsensbasierte Konfigurationen für eine Vielzahl von Technologien, einschließlich Betriebssystemen, Cloud-Diensten und Netzwerkgeräten. Durch die Einhaltung der CIS-Benchmarks können Organisationen ihre Sicherheit verbessern, die Einhaltung gesetzlicher Anforderungen sicherstellen und das Risiko von Sicherheitsverletzungen reduzieren. Nähere Informationen zu CIS-Benchmarks finden Sie hier: CIS-Benchmarks.

- **„Verarbeitung von Daten“**: Gemäß Art 4 Ziffer 2 der Datenschutzgrundverordnung (DSGVO) ist unter der Verarbeitung von (personenbezogenen) Daten jeglicher Vorgang mit den Daten zu verstehen, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung der Daten. Diese Definition wird auch in weiterer Folge in diesem Dokument angewandt.

- **„Need to know“ Prinzip:** Das Prinzip „Kenntnis nur bei Bedarf“ beschränkt die Weitergabe von Informationen auf Personen, die diese zur Erfüllung ihrer spezifischen Arbeitsaufgaben benötigen. Der Zugang zu sensiblen Informationen wird nur jenen gewährt, deren Rollen und Verantwortlichkeiten dies erfordern, um sicherzustellen, dass Informationen geschützt und nur befugtem Personal offengelegt werden.

- **„Least Privilege“ Prinzip:** Das Prinzip „Minimaler Zugriff“ stellt sicher, dass Einzelpersonen nur die minimalen Zugriffsrechte oder Berechtigungen erhalten, die erforderlich sind, um ihre Arbeitsaufgaben zu erfüllen. Es zielt darauf ab, das Risiko von Missbrauch oder unbefugtem Zugriff zu reduzieren, indem nur der Zugang zu den Informationen und Ressourcen gewährt wird, die für die jeweilige Rolle einer Person unbedingt notwendig sind.

- **„Segregation of Duties“ Prinzip:** Das Prinzip „Aufgabentrennung“ beinhaltet die Aufteilung von Verantwortlichkeiten und Aufgaben auf verschiedene Personen oder Abteilungen, um das Risiko von Betrug, Fehlern oder unbefugten Handlungen zu verringern. Im Zusammenhang mit Informationssicherheit stellt es sicher, dass keine einzelne Person die Kontrolle über alle Aspekte eines kritischen Prozesses hat, wodurch das Risiko des Missbrauchs von Informationen minimiert und die internen Kontrollmechanismen gestärkt werden.

4. Allgemeine Sicherheitsvorgaben

ISO27001 1. Der Lieferant muss Änderungen an Systemen oder Infrastruktur, welche A1-Daten verarbeiten, gemäß eines dokumentierten IT-Change Prozesses durchführen.

2. Der Lieferant muss sich im Bedarfsfall nach entsprechender Vorankündigungszeit durch A1 (oder durch einen von A1 akzeptierten Dritten) auditieren lassen.

3. Der Lieferant muss sicherstellen, dass die Serviceerbringung einem definierten Vorgehensmodell für das Service Management (z.B. COBIT, ITIL, ISO 20000) unterliegt.

ISO27001 4. Der Lieferant muss sicherstellen, dass Maßnahmen zur Überprüfung der Vertraulichkeit seiner Mitarbeiter (z.B. durch Backgroundchecks oder Strafregisterauszüge) durchgeführt werden.

5. Die Rechnerstandorte, an denen seitens des Lieferanten und/oder seinen Lieferanten („4th Parties) A1-Daten verarbeitet werden, müssen gegenüber A1 offengelegt werden.

5. Vulnerability & Incident Management

ISO27001 1. Für angebotene Software müssen vom Hersteller Security-Updates/Patches zur Verfügung gestellt werden.

2. Für die Behebung von Sicherheitsschwachstellen der Produkte und Dienstleistungen dürfen vom Lieferanten während der Laufzeit des Wartungsvertrags keine Kosten verrechnet werden.

ISO27001 3. Sicherheitsvorfälle und Datenschutzverletzungen mit potenzieller Auswirkung auf jene Produkte/Dienste, welche A1 vom Lieferanten bezieht und/oder mit potenzieller Auswirkung auf Daten, welche der Lieferant von A1 erhalten hat, müssen unverzüglich (spätestens jedoch innerhalb 20 Stunden nach Kenntnis) an abuse@a1.at und cert@a1.at gemeldet werden. Die Meldung hat jedenfalls folgende Informationen zu enthalten:
   - eine Beschreibung der Art und Umfang des Vorfalls (u.a. Kategorisierung, zeitliche Eingrenzung, betroffene Informationen und Abschätzung des zu erwartenden Impacts),
   - Kontaktpersonen und Informationsmöglichkeiten,
   - bereits ergriffene Maßnahmen beim Lieferanten und Vorschläge, welche Maßnahmen A1 ergreifen soll,
   - oder, falls personenbezogene A1-Daten betroffen sein könnten, sind die Vorgaben der DSGVO zu erfüllen.

4. Schwachstellen müssen gemäß folgender Tabelle adressiert werden (Start ab der Identifizierung der Schwachstelle im System): LOW 90 Tage, MEDIUM 60 Tage, HIGH 30 Tage, CRITICAL 15 Tage. Als Basis für die Klassifizierung dient die Einstufung lt. CVSS v4 (Sollte eine Kategorisierung nach CVSS v4 nicht verfügbar sein, müssen frühere Versionen verwendet werden z.B. CVSS v3, CVSS v2).

5. Der Lieferant muss Systeme und Infrastruktur, die A1-Daten verarbeiten, nach allgemein anerkannten Methoden (z.B. CIS Benchmarks) härten. Auf Verlangen von A1 sind Nachweise über die verwendeten Vorgaben und den Umsetzungsgrad zu erbringen.

6. Der Lieferant muss auf Systemen und Infrastruktur, welche A1-Daten verarbeiten, sicherstellen, dass in regelmäßigen Abständen nachweislich auf Schwachstellen evaluiert wird (z.B. Schwachstellen-Scans, Software-Inventory-Checks, Code & Library-Analysen). Auf Verlangen von A1 sind Nachweise über die Durchführung dieser Evaluierungen zu erbringen.

7. Der Lieferant hat eine Mitwirkungspflicht bei der Aufklärung und Feststellung von sicherheitsrelevanten Vorfällen und muss sicherstellen, dass sicherheitsrelevante Log-Informationen (Admin- und Benutzerverhalten, relevante Kopiervorgänge, etc.) jener Infrastruktur, auf welcher A1-Daten verarbeitet werden, für den Zeitraum von mindestens 18 Monaten existieren und bei Bedarf (z.B. für forensische Analysen) A1 bereitgestellt werden.

ISO27001 8. Der Lieferant muss auf Systemen und Infrastruktur, die A1-Daten verarbeiten, regelmäßige (nach Vorgaben, welche z.B. in Service Level Agreements - SLAs - vereinbart wurden) Datensicherungen durchführen und deren Wiederherstellbarkeit nachweislich testen. Auf Verlangen von A1 sind Nachweise über die Erfüllung dieser Tests zu erbringen.

ISO27001 9. Sofern vom Lieferanten Cloud-Dienste oder sonstige Online-Dienste an A1 geliefert werden, muss er sicherstellen, dass die Systeme und Infrastruktur, die A1-Daten verarbeiten, sicherheitsrelevante Events strukturiert und maschinenlesbar protokollieren sowie vorhalten (Log-Daten). Eine Anbindung an das A1-SIEM muss durch den Lieferanten ermöglicht werden.

ISO27001 10. Der Lieferant muss sicherstellen, dass ein Notfallmanagement für Systeme und Infrastruktur, auf denen A1-Daten verarbeitet werden, geplant, dokumentiert und umgesetzt ist.

11. Der Lieferant muss an Systemen und Infrastruktur, die A1-Daten verarbeiten, regelmäßig und zumindest alle 18 Monate Penetration Tests durchführen lassen sowie Maßnahmen zu gefundenen Schwachstellen ableiten und umsetzen. Nachweise über solche erfolgten Prüfungen muss der Lieferant A1 auf Anfrage bereitstellen. Sollte A1 Zweifel an der Qualität der erfolgten Penetration Tests haben, erklärt sich der Lieferant bereit, sich von A1 oder einem vom Lieferanten akzeptierten Dritten im Auftrag von A1 mittels Penetration Tests prüfen zu lassen.

6. Netzwerksicherheit

1. Security-Updates für IoT-Devices müssen vom Hersteller und/oder Lieferanten über den ganzen Lebenszyklus der Produkte angeboten werden und automatisiert bzw. ohne manuellen Eingriff verteilt und installiert werden können. Es dürfen keine unveränderlichen Passwörter (hardcoded) in den Devices hinterlegt sein.

ISO27001 2. Der Lieferant muss für Systeme und Infrastruktur, die A1-Daten verarbeiten, Sicherheitsmaßnahmen gegen netzbasierte Angriffe (z.B. Intrusion Prevention System - IPS, Firewall, Netzwerksegmentierung) einsetzen.

ISO27001 3. Der Lieferant muss seine Netzwerke, Informationssysteme und User so gruppieren, dass das "Least Privilege"-Prinzip umgesetzt wird.

4. Der Lieferant muss für Systeme und Infrastruktur, die A1-Daten verarbeiten und aus dem Internet erreichbar sind, Maßnahmen zur Verhinderung oder Mitigation von Denial-of-Service (DOS)-Attacken im Einsatz haben. Diese Maßnahmen müssen dokumentiert und auf Verlangen A1 nachgewiesen werden.

ISO27001 5. Der Lieferant muss sicherstellen, dass alle Versorgungskomponenten (z.B. Energieversorgung) redundant ausgelegt sind, sofern sie der Aufrechterhaltung und dem Betrieb von A1-relevanten Systemen dienen.

7. Software-Architektur

ISO27001 1. Der Lieferant muss geeignete Maßnahmen umsetzen, um eine Mandantentrennung zwischen A1 und anderen Kunden des Lieferanten zu gewährleisten. Die Maßnahmen müssen dokumentiert und auf Verlangen von A1 nachgewiesen werden.

ISO27001 2. Der Lieferant muss bei der Entwicklung von Applikationen die Prinzipien einer "Sicheren Software Entwicklung" (z.B. im Software Development Life Cycle - SDLC, Threat Modelling, etc.) einhalten, sowie eine sichere Skalierung und logische Segmentierung der Anwendung aufweisen – beispielsweise durch die Unterteilung der Applikation in Ebenen/Tiers und Microservices.

3. Bei der Unterteilung von Applikationen in Ebenen/Tiers muss der Lieferant sicherstellen, dass beim Zugriff auf Applikationen keine Ebene (Tier) übersprungen werden kann und dass beim Wechsel von einer Ebene (Tier) auf die Nächste nur definierte Protokolle (Ports) verwendet werden.

ISO27001 4. Der Lieferant muss sicherstellen, dass eine Trennung zwischen Präproduktiv- und Produktivsystemen umgesetzt ist.

5. Der Lieferant darf von A1 erhaltene Produktivdaten (Echtdaten) ausschließlich in Produktionsumgebungen verarbeiten und auf Test-/Präproduktiv-Umgebungen nur anonymisierte bzw. synthetische Daten nutzen.

ISO27001 6. Der Lieferant muss für Systeme und Infrastruktur, die A1-Daten verarbeiten, Maßnahmen umsetzen, damit:
- der Zugriff auf Produktivsysteme (Echtdaten) eingeschränkt wird, sowie
- das Prinzip "Need to Know" (Personen mit Zugriffsrechten haben einen legitimen Business Need) und
- das Prinzip "Segregation of Duties"

sichergestellt sind. Dies betrifft vor allem administrative Zugriffe des Lieferanten auf diese Systeme und Infrastruktur.

7. Der Lieferant muss bei der Code-Entwicklung Maßnahmen (z.B. statische/dynamische Sourcecode-Analysen) zur Auffindung von Software-Schwachstellen im Quellcode einsetzen. Die Maßnahmen müssen dokumentiert und auf Verlangen von A1 nachgewiesen werden.

8. Verschlüsselung

ISO27001 1. Die Datenübertragung zwischen der Infrastruktur bzw. den Systemen des Lieferanten und der Infrastruktur bzw. den Systemen von A1 muss verschlüsselt erfolgen.

ISO27001 2. Die Speicherung von A1 Daten auf der Infrastruktur bzw. den Systemen des Lieferanten muss verschlüsselt erfolgen.

ISO27001 3. Der Lieferant muss sicherstellen, dass kryptographische Schlüssel in einer sicheren Umgebung erzeugt, aufbewahrt und archiviert werden.

4. Der Lieferant muss auf Systemen und Infrastruktur, auf denen A1-Daten verarbeitet werden, zu jeder Zeit sicherstellen, dass nur Verschlüsselungsmethoden eingesetzt werden, die als 'State of the Art' gelten (wie z.B. AES mit einer Schlüssellänge von 128-256 Bit, Camellia mit 128-256 Bit, ECIES mit >250 Bit, DLIES mit >3000 Bit, RSA mit >3000 Bit).

ISO27001 5. Der Lieferant muss auf Systemen und Infrastruktur, auf denen A1-Daten verarbeitet werden, sicherstellen, dass keine Verschlüsselungsmethoden verwendet werden, die als veraltet gelten (wie z.B. Triple-DES, Serpent, Twofish, DES, RC4, Blowfish).

6. Der Lieferant muss mit seinen Lieferanten („4th Parties“) vereinbaren, dass die Datenübertragung zwischen ihm und diesen Lieferanten („4th Parties“) verschlüsselt erfolgt.

7. Der Lieferant muss sicherstellen, dass für A1-relevante Systeme:
- regelmäßige Wechsel von kryptografischen Schlüsseln technisch unterstützt durchgeführt werden können,
- Prozesse zum Schlüsselwechsel etabliert sind sowie,
- Schlüsselwechsel auf Verlangen von A1 (durch den Lieferanten) durchgeführt werden bzw.
- Schlüsselwechsel eigenständig von A1 durchgeführt werden können.

Die Durchführung muss dokumentiert und auf Verlangen von A1 nachgewiesen werden.

9. Authentifizierung und Berechtigungsmanagement

1. Eine Authentisierung am System des Lieferanten über eine A1-seitig vorhandene Single-Sign-On-Lösung (SSO, z.B. Active Directory Federation Services - ADFS) muss – jedenfalls ab einer Userzahl von 50 - technisch möglich sein.

2. Falls die Lösung des Lieferanten lokale Benutzerkonten erfordert, muss die Benutzerverwaltung (anlegen, löschen, sperren, ändern) durch A1 möglich sein.

3. Der Lieferant muss sicherstellen, dass auf seinen Systemen und seiner Infrastruktur, auf denen A1-Daten verarbeitet werden, Benutzerrechte und -rollen vergeben/entzogen werden können. Mittels dieser Information muss es A1 möglich sein, regelmäßige Prüfungen sowie Änderungen der Benutzerrechte und -rollen durchzuführen.

4. Falls die Lösung des Lieferanten lokale Benutzerkonten erfordert, müssen die folgenden Vorgaben für sichere Passwörter erfüllt werden:
   - Erfordern eine Mindestlänge von 15 Zeichen,
   - Erfordern mindestens 3 dieser 4 Kriterien: Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen,
   - Regelmäßige und/oder spontane Passwortwechsel müssen technisch unterstützt werden und
   - Eine Passwortspeicherung und -übertragung im Klartext ist nicht zulässig.

5. Biometrische Authentifizierung:
   - Bei biometrischer Authentifizierung müssen die Authentifizierungsdaten ausschließlich lokal und sicher am jeweiligen Gerät gespeichert werden und dürfen nicht mit Standard-Rechten (beispielsweise von der Festplatte) auslesbar sein.
   - Bei Verfahren zur Gesichtserkennung müssen Kriterien wie Dreidimensionalität oder Temperatur mitgeprüft werden.
   - Bei Verfahren zum Fingerabdruck-Scanning müssen Kriterien wie Fingerpuls oder Temperatur mitgeprüft werden.
   - Die Falschakzeptanzrate (unberechtigte User werden autorisiert) muss bei maximal 1 zu 50.000 liegen.
   - Die Falschrückweisungsrate (berechtigter User wird nicht autorisiert) muss in einem akzeptablen Rahmen sein.
   - Um sich bei einer Falschrückweisung trotzdem authentifizieren zu können, muss alternativ ein Passwortschutz gemäß den oberen Angaben möglich sein.

6. Alternative Authentifizierungsmethoden sind zulässig, sofern sie ein gleich- oder höherwertiges Schutzniveau zu den sonstigen in diesen Vorgaben beschriebenen Verfahren aufweisen. Die Zustimmung von A1 zu einer alternativen Authentifizierungsmethode muss eingeholt werden.

7. Der Lieferant muss sicherstellen, dass folgende Anforderungen an Initialpasswörter erfüllt sind:
   - Müssen zufallsbedingt erzeugt werden,
   - Werden verschlüsselt übertragen,
   - Können nur ein einziges Mal eingesetzt werden und
   - Dürfen nur maximal 14 Tage gültig sein.

8. Der Lieferant muss sicherstellen, dass bei personenbezogenen Accounts, nach dem Ersteinstieg mittels Initialpasswort sofort ein Passwortwechsel erzwungen wird und es im Bedarfsfall (beispielsweise nach einem Incident) möglich ist, die Anmeldeinformation zu ändern.

9. Der Lieferant muss geeignete Maßnahmen zur Verhinderung unberechtigter Zugriffe umsetzen (z.B., dass nach mehreren fehlgeschlagenen Versuchen der Zugriff für eine bestimmte Zeit unterbunden wird, um Bruteforce-Angriffen vorzubeugen). Die Maßnahmen müssen dokumentiert und auf Verlangen von A1 nachgewiesen werden.

10. Reporting

1. Ein quartalsweises Reporting des Lieferanten an den Service-Verantwortlichen innerhalb der A1 über die erbrachten Leistungen muss erfolgen und mindestens folgende Punkte beinhalten:
   - Verfügbarkeit des Systems kalendermonatlich,
   - Incident Reaction Time,
   - Incident Resolution Time kalendermonatlich,
   - Durchgeführte technische Security Maßnahmen,
   - Gefundene Schwachstellen nach CVSS-Klassifizierung,
   - Behobene Schwachstellen sowie
   - Behebungszeiten für Schwachstellen.

11. Malwareschutz und Reaktionsmöglichkeiten

ISO27001 1. Es muss eine Endpoint-Security-Lösung (z.B. eine Antivirus-Software) im Einsatz sein, welche laufend die Systeme und Dateien auf Schadsoftware (z.B. Ransomware, Malware) überprüft. Die Endpoint-Security-Lösung muss laufend aktualisiert werden sowie eine Echtzeitüberwachung und Reaktion ermöglichen. Identifizierte Schadsoftware muss unverzüglich entfernt werden.

12. Physische Sicherheit

ISO27001 1. Der Lieferant muss geeignete Maßnahmen ergreifen, um den physischen Zutritt zu seinen Büroräumlichkeiten sowie Betriebsräumen zu überwachen. Die Maßnahmen müssen dokumentiert und auf Verlangen von A1 nachgewiesen werden.

ISO27001 2. Der Lieferant muss sicherstellen, dass sich Systeme und Infrastruktur, auf denen A1-Daten verarbeitet werden, in zutrittsgesicherten Bereichen befinden.

13. Deprovisionierung & Datenlöschung

ISO27001 1. Zu Vertragsende müssen sämtliche A1-relevante Daten vom Lieferanten an A1 (unter Berücksichtigung sonstiger vertraglicher Pflichten mit A1 sowie der dargelegten Löschpflichten in Kontrolle 12.2) übergeben werden. Die Übergabe muss in einem gängigen und für A1 lesbaren Format erfolgen.

2. Der Lieferant muss sicherstellen, dass A1-Daten (sofern sie nicht mehr zur Erfüllung der vertraglichen Pflichten benötigen werden und die Übergabepflicht aus Kontrolle 12.1 erfüllt wurde) gelöscht werden. Dies kann durch mehrmaliges Überschreiben der Daten, durch die Vernichtung kryptographischen Schlüssel oder zertifizierte Zerstörung der Datenträger erreicht werden. Auf Verlangen ist A1 ein Nachweis über die erfolgte Datenlöschung vorzulegen.

14. Continuity Management

1. Der Lieferant muss Notfallpläne für A1-relevante Systeme erstellen, regelmäßig bewerten und testen. Die Notfallpläne müssen dokumentiert und A1 auf Verlangen nachgewiesen werden.

15. Cloud- oder sonstige Online-Dienste

ISO27001 1. Der Lieferant muss sicherstellen, dass Cloud- oder sonstige Online-Dienste redundant an mindestens 2 Rechenzentren-Standorten betrieben werden.

ISO27001 2. Der Lieferant muss sicherstellen, dass alle A1-relevanten Komponenten von seinen Cloud- oder sonstigen Online-Diensten in ein zentrales Konfigurationsmanagementsystem eingebunden sind.

16. Inhaltliche Verantwortung

	Der Inhalt wurde erstellt von: A1 OneSEC (Austria) Security@A1.at

17. Versionshistorie

„A1 Minimum Sicherheitsanforderungen für Lieferanten" - Version 1.1
Changelog: • Harmonisierung der Versionsbezeichnung (beide auf Version 1.1) zwischen dem Dokument in Deutsch an das Dokument in Englisch aufgrund dortiger Änderungen
„A1 Minimum Sicherheitsanforderungen für Lieferanten" - Version 1.0
Changelog: • Neuerstellung des Dokuments durch komplette Überarbeitung/Konsolidierung des Dokuments „A1 Standard für den sicheren Servicebetrieb".

18. Anhang A: Mapping zu den ISO 27001:2022 Kontrollen

Kapitel- und Kontrollnummer	ISO 27001:2022	
	Mit ISO-Zertifizierung abgedeckt	A1-spezifische Anforderung mit Verweis auf relevantes ISO-Kapitel
4. Allgemeine Sicherheitsvorgaben		
4.1	8.32	
4.2		8.34
4.3		5.22
4.4	6.1	
4.5		7.9
5. Vulnerability & Incident Management		
5.1	7.13, 8.8, 8.30	
5.2		Ohne
5.3	5.24	
5.4		8.8, (8.30)
5.5		5.36, 8.9, 8.16, 8.20, 8.26
5.6		5.19, 5.20, 5.21, 5.22, 8.8
5.7		5.19, 5.20, 5.21, 5.22, 8.15
5.8	5.19, 5.20, 5.21, 5.22, 5.24, 5.25, 5.26, 5.27, 5.29, 5.30, 5.31, 5.33, 8.13, 8.14	
5.9	8.15, 8.16	
5.10	5.24, 5.25, 5.26, 5.27, 5.28, 5.30	
5.11		5.35, 8.34
6. Netzwerksicherheit		
6.1		7.13
6.2	8.20, 8.21, 8.22, 8.23	
6.3	8.2, 8.22	
6.4		8.6, 8.14, 8.16, 8.20, 8.21
6.5	7.11, 8.14	
7. Software-Architektur		
7.1	5.23, 8.21, 8.22, 8.27	
7.2	8.25, 8.27, 8.28	
7.3		8.25, 8.27, 8.28
7.4	8.22, 8.31	
7.5		8.11
7.6	8.2, 8.3	
7.7		8.28, 8.29, 8.30
8. Verschlüsselung		
8.1	8.24	
8.2	8.24	
8.3	5.33, 8.24	
8.4		8.24
8.5	5.14, 5.19, 5.20, 5.21, 8.20, 8.24	

8.6		8.24, 8.27
9. Authentifizierung und Berechtigungsmanagement		
9.1		8.5
9.2		5.15, 5.16, 5.17, 5.18, 8.5
9.3		5.2, 5.18, 8.2, 8.3
9.4		5.17, 8.5, 8.24, 8.27
9.5		8.1, 8.5
9.6		8.5
9.7		8.5, 8.24, 8.27
9.8		5.17, 5.26, 8.5, 8.27
9.9		8.5
10. Reporting		
10.1		5.21, 5.24, 5.26, 5.28, 6.8
11. Malwareschutz und Reaktionsmöglichkeiten		
11.1	8.1, 8.7	
12. Physische Sicherheit		
12.1	5.15, 5.18, 7.2, 7.3, 7.4	
12.2	5.15, 5.18, 7.2, 7.3, 7.8	
13. Deprovisionierung & Datenlöschung		
13.1	5.11, 5.23	
13.2		5.11, 5.23, 8.24
14. Continuity Management		
14.1		5.24, 5.25, 5.29, 5.30
15. Cloud- oder sonstige Online-Dienste		
15.1	5.30, 8.14	
15.2	5.9, 8.9	