Sicherheitsanforderungen für Lieferanten der EVN Gruppe

Version 1.0

Gültig ab: 21.3.2022

EVN Informationsklassifikation: öffentlich

Versorgungssicherheit und sichere Dienstleistungen sind ein wesentlicher Bestandteil unserer Unternehmensstrategie. Die Zusammenarbeit mit unseren Partnern und Lieferanten ist essentiell, um erfolgreich Informations-Sicherheitsanforderungen umzusetzen. Es ist uns wichtig, Daten, Systeme und Anwendungen mit Sicherheitsmaßnahmen nach führenden Industriestandards zu schützen, wie es von einem der führenden österreichischen Konzerne im Energie- und Umweltsektor erwartet wird. Das Management von Lieferantenbeziehungen in Bezug auf die Sicherheit ist ein wichtiger Teil des internen Risikomanagements, eine gängige Praxis nach internationalen Standards (z.B. ISO 27000-Serie, NIST Cybersecurity Framework) und für Unternehmen im Bereich der kritischen Infrastruktur bzw. als Anbieter wesentlicher Dienste kann diese auch gesetzlich verpflichtend sein (z.B.: NIS Gesetz).

Der Bieter, Auftragsverarbeiter, Auftragnehmer oder Vertragspartner (in weiterer Folge als „Lieferant" bezeichnet) der EVN Gruppe (EVN AG und der mit ihr verbundenen Unternehmen, in weiterer Folge als „EVN“ bezeichnet) sichert zu und gewährleistet, dass er alle erforderlichen Sorgfaltspflichten erfüllt hat, mit den gestellten Sicherheitsanforderungen vertraut ist, diese anerkennt und sich verpflichtet, sie auch einzuhalten, wenn er:

(a) auf Einrichtungen, Netzwerk und/oder Informationssysteme der EVN zugreift oder

(b) auf Informationen/Daten der EVN zugreift, diese verarbeitet oder speichert oder

(c) IT-Infrastrukturdienste und/oder Standardsoftware bereitstellt oder Software entwickelt.

Wann immer in dieser Sicherheitsanforderung von "Auftraggeber" die Rede ist, sind sinngemäß nicht nur die jeweiligen Daten (bzw. Systeme, Services, etc.) der EVN, sondern auch die ihrer Kunden und Partner zu verstehen. Zusätzliche Sicherheitsanforderungen können in Einzelvereinbarungen (z.B.: SLA, Anforderungskatalog) festgelegt werden. Diese Sicherheitsanforderung ergänzt die Bestimmungen zur Geheimhaltung und Sicherheit in den allgemeinen Einkaufsbedingungen der EVN Gruppe. Einzelvereinbarungen zwischen Lieferant und Auftraggeber, welche die gesamte oder einzelnen Teile dieser Vereinbarung ersetzen oder ergänzen, gehen dieser Vereinbarung vor.

Inhalt

1 Governance

1.1 Richtlinien

Der Lieferant unterhält ein Managementsystem für die Informationssicherheit, das einen kontinuierlichen Verbesserungsprozess auf der Grundlage anerkannter Standards umfasst.

Informationssicherheitsrichtlinien, -verfahren, -rollen, -verantwortlichkeiten und -zuständigkeiten werden in Übereinstimmung mit den Geschäftsanforderungen des Lieferanten und den einschlägigen Gesetzen, Vorschriften und gängigen Sicherheitsstandards festgelegt. Die Informationssicherheitsrichtlinien werden von der Geschäftsleitung genehmigt, veröffentlicht und an die Mitarbeiter und relevanten externen Parteien weitergegeben.

Der Lieferant überprüft regelmäßig, ob er die festgelegten Informationssicherheitsrichtlinien und -standards sowie alle anderen Informationssicherheitsanforderungen einhält.

1.2 Risikomanagement

Der Lieferant verfügt über ein Informationssicherheitsrisikomanagement. Der Lieferant stellt sicher, dass Risiken, die sich direkt oder indirekt auf die Dienste und/oder Daten des Auftraggebers auswirken, bewertet und Maßnahmen zur Risikominderung ergriffen und dokumentiert werden. Risiken, die den Auftraggeber direkt oder indirekt betreffen, müssen auf Verlangen gemeldet werden.

1.3 Klassifizierung von Informationen

Unterschiedliche Informationen haben einen unterschiedlichen Bedarf nach Vertraulichkeit. Die Vertraulichkeitsklassen können als Maß dafür gesehen werden, welche Auswirkungen ein Missbrauch der Information haben kann. Überlässt der Auftraggeber dem Lieferant Informationen, so ist nach folgender Kategorisierung vorzugehen. Dabei wird nach 4 Gruppen kategorisiert, die den Umgang mit den jeweiligen Informationen regeln. Die Farbkennzeichnung basiert auf dem international üblichen Traffic Light Protocol (TLP).

Vertraulichkeitsklasse	**Farbkennzeichnung**
Öffentlich	weiß (white)
Intern	grün (green)
Vertraulich	orange (amber)
Streng vertraulich	rot (red)

1.4 Vertragliche Vereinbarungen

Der Lieferant muss die Verantwortung für die Informationssicherheit in die vertraglichen Vereinbarungen mit seinen Mitarbeitern und Auftragnehmern aufnehmen.

1.5 Hintergrund-Checks

Die Überprüfung des Hintergrunds von Bewerbern für eine Beschäftigung erfolgt in Übereinstimmung mit den einschlägigen Gesetzen und Vorschriften. Der Umfang der Überprüfung muss im Verhältnis zu dem mit der Funktion des Bewerbers verbundenen Risiko stehen.
Beispiel: In Österreich Strafregisterbescheinigung oder ähnliche Prüfmechanismen in anderen Ländern (criminal record extract).

1.6 Sensibilisierungsprogramm

Alle Mitarbeiter des Lieferanten und gegebenenfalls auch die Auftragnehmer erhalten eine ihrer Funktion entsprechende Sensibilisierung und Schulung. Darüber hinaus werden die Mitarbeiter auch über Aktualisierungen der Richtlinien und Verfahren des Lieferanten unterrichtet. Das gesamte Personal muss über die für seine Aufgaben und Zuständigkeiten erforderlichen Kenntnisse verfügen.

2 Change Management

2.1 Asset-Lebenszyklus

Der Lieferant stellt sicher, dass die Informationssicherheit ein integraler Bestandteil der Informationssysteme über deren gesamten Lebenszyklus ist (Erwerb bis Stilllegung und Entsorgung der Anlagen und Systeme). Der Lieferant stellt sicher, dass die bereitgestellten Komponenten und deren Betriebssysteme, Middleware (z.B. Java) und Applikationen unterstützt werden, und aktuelle Sicherheitsupdates erhalten. Der Lieferant sorgt für regelmäßige, rechtzeitige Sicherheitsupdates während des gesamten Vertragslebenszyklus.

Der Lieferant stellt sicher, dass ihm überlassene Komponenten (z.B.: Geräte, Medien) nach Beendigung des Vertragsverhältnisses dem Auftraggeber retourniert werden.

2.2 Software Change Management

Der Lieferant verfügt über formale Richtlinien für das Change-Management und den Lebenszyklus der sicheren Softwareentwicklung, die auch sicherheitsrelevante Kontrollen festlegen. Überprüfungen der Cybersicherheit bei neuen Systemdesigns oder Änderungen an Systemen sowie Sicherheitstests vor der Bereitstellung müssen Teil der Prozesse sein. Änderungen werden in angemessener Weise angefordert, autorisiert, getestet und genehmigt, bevor sie für die Produktion freigegeben werden.

2.3 Lebenszyklus der sicheren Softwareentwicklung

Der Lieferant nimmt Aspekte der Informationssicherheit in die Produkt-Dokumentation auf. Diese Dokumentation muss Anweisungen für die Konfiguration des Dienstes und/oder der Umgebung enthalten, um einen sicheren Betrieb zu gewährleisten. Entwickelte Software muss in einer kontrollierten Umgebung getestet werden, um Schwachstellen zu erkennen, bevor sie dem Auftraggeber zur Verfügung gestellt wird.

Der Lieferant stellt sicher, dass der Lebenszyklus der Softwareentwicklung angemessene Sicherheitsmaßnahmen enthält (Secure Software Development Lifecycle). Dies beinhaltet, ist aber nicht beschränkt auf:

- → Einsatz international anerkannter, sicherer Softwareentwicklungsmethoden (einschließlich agiler Prozesse wie Scrum, Kanban, etc.) als integraler Bestandteil des sicheren Softwareentwicklungsprozesses
- → Sichere Coding-Richtlinien auf der Grundlage internationaler Normen.
- → Die Integrität des Quellcodes ist gewährleistet.
- → Regelmäßige Überprüfung des sicheren Codes (statische und dynamische Anwendungssicherheitstests)
- → Schwachstellen-Scans, die auch den verwendeten Code von Drittanbietern und Open-Source-Komponenten (z.B. Bibliotheken) umfassen
- → Sicherheits- und Penetrationtests, die von einer unabhängigen dritten Partei durchgeführt werden
- → Angemessene Schulungen für interne und externe Softwareentwickler.
- → Gefundene und bekannte Schwachstellen werden vor der Freigabe für die Produktion beseitigt.

3 Outsourcing

3.1 Sub-Outsourcing

Der Lieferant hat klare vertragliche Vereinbarungen mit allen Unterauftragnehmern von Dienstleistungen, um deren Verantwortung für die Sicherheit der Daten des Auftraggebers, die sie im Auftrag des Auftraggebers verarbeiten / speichern / übermitteln, festzulegen. Der Lieferant stellt sicher, dass die von den Unterauftragnehmern eingeführten Sicherheitsmaßnahmen mindestens das in diesem Dokument und im Hauptvertrag angegebene Niveau haben. Der Lieferant prüft die Wirksamkeit der Maßnahmen im Rahmen seines Lieferantenmanagementprozesses.

4 Sicherer Systembetrieb

4.1 Identitäts- und Zugriffsmanagement

Der Lieferant hat Zugriffskontrollen eingerichtet, um Identitäten zu überprüfen und den Zugriff auf autorisierte Benutzer zu beschränken. Die Zugriffsrechte beruhen auf dem Prinzip des minimalen Zugriffs und der dienstlichen Erforderlichkeit des Zugriffs. Darüber hinaus wird der Grundsatz der "Aufgabentrennung" beachtet.

Der Lieferant hat Authentifizierungsmechanismen implementiert, um den Zugriff zu den Systemen nach bewährten Verfahren zu schützen, die unter anderem Folgendes umfassen:

- → Passwortrichtlinien (12 Zeichen Mindestlänge, Komplexität, Vermeidung von Wiederverwendung)
- → eindeutige Benutzeridentifikation (generische und gemeinsame Benutzer werden vermieden)
- → Sichere Speicherung/Verwaltung/Übermittlung von Anmeldedaten

Der Lieferant stellt sicher, dass Konten, die für den Zugriff über das Internet genutzt werden, durch starke Authentifizierungsmechanismen, zumindest Multi-Faktor Authentifizierung, geschützt sind.

Der Lieferant hat strenge Kontrollen für privilegierte Konten (z.B. Systemadministratoren) durch starke Authentifizierung (z.B. Multi-Faktor Authentifizierung), Beschränkung auf ein Minimum und streng überwachte Nutzung eingeführt.

Der Lieferant überprüft die Zugriffsrechte seiner Mitarbeiter in regelmäßigen Abständen und ändert (d.h. beschränkt/widerruft) sie, falls erforderlich. Der Lieferant informiert den Auftraggeber bei Kündigung oder Beendigung des Dienstverhältnisses von zugriffsberechtigten Mitarbeitern. Alle Zutrittsmittel (z.B.: Schlüssel, Zutrittskarten, Fernzugriffs-Token) sind dem Auftraggeber unverzüglich zu retournieren.

4.2 Patch Management

Der Lieferant analysiert regelmäßig die Systeme (Betriebssysteme, Anwendungen, Netzkomponenten) auf bekannte Schwachstellen. Patches werden in einer konsistenten, standardisierten Weise angewendet und nach ihrer Kritikalität priorisiert. Wenn die Ursache von Schwachstellen nicht innerhalb eines angemessenen Zeitraums beseitigt werden kann, müssen bis zur Behebung alternative Maßnahmen zur Risikominderung ergriffen werden. Der Lieferant hat einen Notfall-Changeprozess implementiert.

4.3 Netzwerksicherheit

Der Lieferant hat Komponenten der Netzsicherheitsinfrastruktur wie Firewalls, Intrusion Detection/Prevention Systeme (IDS/IPS) oder andere Sicherheitskontrollen implementiert und aufrechterhalten, die eine Erkennung, kontinuierliche Überwachung und eine Einschränkung des Netzwerkverkehrsermöglichen, um die Auswirkungen von Angriffen zu begrenzen. Für Systeme mit einer höheren Risikostufe (z.B. für einen Zugriff von externen Netzwerken erreichbar) müssen strengere Maßnahmen ergriffen werden.

Der Lieferant stellt sicher, dass eine formelle Fernzugriffsrichtlinie vorhanden ist.

Fernzugriffe des Lieferanten auf Netzwerke und Systeme des Auftraggebers sind nur unter den durch den Auftraggeber gesondert bekanntgegebenen Bedingungen und Sicherheitsvorgaben sowie nach Abschluss einer gesonderten Fernzugriffsvereinbarung gestattet.

Der Lieferant stellt die Trennung und Segmentierung der Umgebungen gemäß den Industriestandards sicher, wenn:

(1) Umgebungen gemeinsam mit anderen Kunden genutzt werden; und/oder
(2) der Lieferant Test-, Qualitäts- und Produktionsumgebungen einrichtet.

4.4 Verschlüsselung

Der Lieferant gewährleistet einen angemessenen Schutz der Vertraulichkeit der Daten. Der Lieferant muss auch spezifische Maßnahmen für Daten bei der Übertragung sowie in flüchtigen und persistenten Speichern berücksichtigen, wie z. B. die Verwendung von Verschlüsselungstechnologien in Kombination mit einer geeigneten Schlüsselverwaltungs-architektur. Die Verschlüsselung entspricht den führenden Standards und Richtlinien oder gleichwertigen Standards (z.B. National Institute of Standards and Technology - NIST).

Der Lieferant schützt mobile Geräte und externe elektronische Medien (z.B. USB-Speicher, tragbare Festplatten, Band) durch angemessene physische und logische Sicherheitsmaßnahmen vor unbefugtem Zugriff. Die Verschlüsselung von auf diesen Geräten gespeicherten Daten muss durchgesetzt werden.

4.5 Schutz vor Schadsoftware

Der Lieferant schützt die Server und Endgeräte mit einem angemessenen Schutz vor Malware, der stets auf dem neuesten Stand gehalten wird. Die Software muss erkennen, ob die Antiviren-/Malware-Software auf den Geräten deaktiviert wurde oder nicht regelmäßig aktualisiert wird.

4.6 Sicherheitsüberprüfung & Überwachung

Der Lieferant verfügt über angemessene Sicherheitsmaßnahmen (insbesondere im Hinblick auf Cyber-Bedrohungen) für Daten, Anwendungen und Systeme. Der Lieferant evaluiert regelmäßig die Wirksamkeit der Sicherheitsmaßnahmen in Bezug auf bekannte Cyber-Bedrohungen und Betrugsfälle sowie entsprechende Modelle (z.B. auf der Grundlage aktueller Bedrohungskataloge wie National Institute of Standards and Technology, Bundesamt für Sicherheit in der Informationstechnik).

Der Lieferant plant und führt in regelmäßigen Abständen Schwachstellenanalysen und Penetrationstests für die Systeme durch, die zur Erbringung der Dienstleistung für den Auftraggeber eingesetzt werden. Penetrationstests für diese Systeme müssen in folgender Weise durchgeführt werden:

(1) mindestens einmal pro Jahr
(2) im Falle einer größeren Release/Aktualisierung von Anwendungen/Software/Informations-diensten
(3) Penetrationstests werden von Testern mit ausreichenden Kenntnissen, Fähigkeiten und Erfahrungen durchgeführt, die nicht an der Entwicklung der Sicherheitsmaßnahmen beteiligt waren.

Die aufgedeckten Schwachstellen und die Ergebnisse müssen in geeigneter Weise verwaltet werden: Analyse, Klassifizierung und Behebung. Die Abhilfemaßnahmen müssen entsprechend ihrer Kritikalität zeitnah durchgeführt werden. Der Lieferant muss auf Anfrage zusammenfassende Ergebnisberichte von Schwachstellenbewertungen und/oder Penetrationstests zur Verfügung stellen.

Der Lieferant stellt sicher, dass vom Auftraggeber gemeldete Sicherheitsprobleme innerhalb eines angemessenen Zeitrahmens behoben werden.

Der Auftraggeber behält sich das Recht vor, Sicherheitsbewertungen und Sicherheitsüberprüfungen durchzuführen, um die Einhaltung der hier aufgeführten Anforderungen zu überprüfen. Der Auftraggeber benachrichtigt den Lieferanten im Voraus und stellt sicher, dass das Audit während der normalen Geschäftszeiten und mit minimaler Unterbrechung des Geschäftsbetriebs des Lieferanten durchgeführt wird. Auf Anfrage muss der Lieferant die Einhaltung der hier aufgeführten Anforderungen schriftlich bestätigen und alle Fragen des Auftraggebers an den Lieferanten zu seinen Sicherheitsverfahren schriftlich beantworten.

4.7 System Hardening

Der Lieferant konfiguriert und setzt seine IT-Ressourcen (z.B. Datenbanken, Anwendungen, Betriebssysteme, Netzwerkgeräte) unter Verwendung einer sicheren Grundlage (Hardening) ein. Die Sicherheitsgrundlagen basieren auf Best Practices (z.B. CIS-Standards) oder gleichwertigen Verfahren. Die Konfigurationen für die IT-Anlagen werden regelmäßig überprüft und aktualisiert.

5 Betrieb

5.1 Data Management

Der Lieferant stellt sicher, dass Maßnahmen gegen Datenverlust und -abfluss getroffen werden.

Der Lieferant darf keine Produktionsdaten des Auftraggebers replizieren oder in Nicht-Produktionsumgebungen verwenden. Jede Verwendung von Daten des Auftraggebers in Nicht-Produktionsumgebungen bedarf der ausdrücklichen, dokumentierten Zustimmung des Auftraggebers.

Der Lieferant stellt sicher, dass Informationen (physisch, digital) bzw. Informationsträger nach Beendigung des Vertragsverhältnisses nach Anforderung sicher gelöscht oder retourniert werden.

5.2 Backup & Recovery

Der Lieferant stellt sicher, dass für jede relevante Plattform/Komponente im Verantwortungsbereich des Lieferanten Sicherungs- und Datenhaltungskonzepte existieren. Backups, Aufbewahrungsfristen und Wiederherstellungstests werden durchgeführt. Die Sicherungskonzepte und Wiederherstellungsverfahren sind geeignet, die vereinbarten Verfügbarkeitsstufen zu gewährleisten.

5.3 Logging & Monitoring

Der Lieferant hat geeignete Maßnahmen ergriffen, um die Nachvollziehbarkeit und Rückverfolgbarkeit der durchgeführten Vorgänge zu gewährleisten. Die Protokolle müssen ausreichende Angaben enthalten, um die Ursache eines (Sicherheits-)Problems zu ermitteln und die Wiederherstellung einer Reihe von Ereignissen zu ermöglichen. Die Protokolle müssen dem Auftraggeber zur Verfügung gestellt werden, wenn der Auftraggeber berechtigte Gründe hat. In den Protokollen müssen Zugriffsversuche, Informationen über System- und Netzsicherheitsereignisse, Warnungen, Ausfälle und Fehler aufgezeichnet werden. Die Integrität der Protokolldateien muss gewährleistet sein. Der Zugang zu den Protokolldateien muss eingeschränkt werden.

5.4 Incident Management & Reporting

Der Lieferant muss über dokumentierte Verfahren für Informationssicherheitsvorfälle verfügen, die eine wirksame und ordnungsgemäße Handhabung von Sicherheitsvorfällen ermöglichen. Die Verfahren müssen die Meldung, Analyse, Überwachung, Lösung und Dokumentation von Sicherheitsvorfällen und Reaktions- und Wiederherstellungsprozesse nach einem Sicherheits-Vorfall umfassen.

Der Lieferant benachrichtigt den Auftraggeber unverzüglich nach Bekanntwerden eines Vorfalls, der direkt oder indirekt mit den Diensten und Daten des Auftraggebers zusammenhängt, per Mail an supplier-incident@evn.at, und stellt alle ihm bekannten Informationen zur Verfügung, um den Auftraggeber bei der Erfüllung seiner Verpflichtungen zu unterstützen. Der Lieferant stellt diese Informationen schrittweise zur Verfügung, sobald sie verfügbar werden. Nach der Überprüfung eines Sicherheitsvorfalls in Verbindung mit den Diensten oder Daten des Auftraggebers wird der Lieferant:

i. die Geschäftsbereiche des Auftraggebers zusätzlich schriftlich benachrichtigen.
ii. Die Meldung hat mindestens folgende Angaben zu enthalten, wenn zunächst nicht alle Informationen vorliegen, sollte der Lieferant die Angaben bei zeitkritischen Fällen oder Gefahr im Verzug sofort nach Bekanntwerden in einer gestaffelten Meldung nachliefern:

   - → Kontaktinformationen der Person beim Lieferanten, die für den Vorfall verantwortlich ist- Was ist passiert?
   - → Wie ist es passiert?
   - → Warum ist es geschehen?
   - → Betroffene Komponenten/Systeme/Anlagen
   - → Betroffene Dienste/Daten des Auftraggebers
   - → Datum und Uhrzeit des Auftretens des Vorfalls
   - → Datum und Uhrzeit der Entdeckung des Vorfalls
   - → Auswirkung auf das Geschäft / Auswirkungen auf Services/ -Daten des Auftraggebers
   - → Lösung des Vorfalls
   - → Ergriffene Maßnahmen zur Behebung des Vorfalls
   - → Geplante Maßnahmen zur Behebung des Vorfalls

iii. alle angemessenen Anstrengungen zu unternehmen, um solche Vorfälle zu entdecken und zu vermeiden;
iv. den Auftraggeber laufend über die Maßnahmen zu informieren, die der Lieferant ergreift oder zu ergreifen beabsichtigt;
v. die vorherige schriftliche Zustimmung des Auftraggebers gemäß dem anwendbaren Recht in Verbindung mit jeglicher Benachrichtigung oder öffentlichen Information in Bezug auf eine solche Verletzung einzuholen, und
vi. alle weiteren Aktivitäten mit dem Auftraggeber zu koordinieren.
vii. diese Meldepflicht gilt auch für Unterauftragnehmer.

6 Physische Sicherheit

6.1 Physischer Zugang

Der Lieferant hat seine Räumlichkeiten in verschiedene Schutzzonen eingeteilt, welche Sicherheitsmaßnahmen und Zugangsrechte gemäß den jeweiligen Sicherheitsanforderungen widerspiegeln.

Der physische Zugang zu IT-Systemen wie z.B. Servern ist durch spezielle Schutzzonen, die nur für befugtes Personal zugänglich sind, weiter eingeschränkt.

7 Business Continuity Management

7.1 BCM

Der Lieferant verfügt über aktuelle und aufrechterhaltene Notfallpläne und Pläne zur Aufrechterhaltung des Geschäftsbetriebs. Die Disaster-Recovery-Pläne und Business-Continuity-Pläne müssen so konzipiert sein, dass negative Auswirkungen durch ungeplante Unterbrechungen so weit wie möglich verhindert werden und dass der Lieferant auch bei Betriebsunterbrechungen weiterarbeiten und die Dienstleistungen gemäß dem Vertrag mit dem Auftraggeber erbringen kann. Der Lieferant stellt dem Auftraggeber auf Anfrage schriftliche Zusammenfassungen seiner Disaster-Recovery-Pläne und Business-Continuity-Pläne zur Verfügung.

Der Lieferant führt mindestens einmal jährlich angemessene Tests seiner eigenen Business-Continuity- und Disaster-Recovery-Pläne durch. Servicerelevante Testergebnisse sind dem Auftraggeber auf Verlangen, zumindest aber nach Durchführung der Tests zur Verfügung zu stellen.

Der Lieferant hat sichergestellt, dass der Geltungsbereich der Business Continuity- und Notfallwiederherstellungspläne alle Standorte, Mitarbeiter und Informationssysteme umfasst, die zur Erbringung von Dienstleistungen für den Auftraggeber eingesetzt werden.