1 Zweck

1.1 Umfang

Die vorliegenden Informationssicherheitsanforderungen und -bestimmungen gelten für Lieferanten (Auftragnehmer) der Wien Energie GmbH. Unter Lieferanten werden in diesem Dokument auch Dienstleister und Hersteller verstanden, sie werden im weiteren als Auftragnehmer (AN) bezeichnet. Der Betreiber des Systems oder der kritischen Infrastruktur wird als Auftraggeber (AG) bezeichnet.

Zweck dieses Dokuments ist es, die wichtigsten Sicherheitsanforderungen an die Lieferanten von Produkten oder Dienstleistungen für die Wien Energie GmbH zu identifizieren und in Form einer Vereinbarung mit den AN zu dokumentieren.

1.2 Ziel

Die Vorgaben dieses Dokuments sind für alle Neuanschaffungen, Erweiterungen, bzw. Umbauten oder Adaptionen (Upgrades, etc.) oder Dienstleistungen an bestehenden IKT-Systemen und IT/OT-Komponenten, die Daten und Informationen verarbeiten, weiterleiten, empfangen oder speichern, anzuwenden. Sie richtet sich an interne wie auch externe Lieferanten der Wien Energie GmbH

Da jedes System unterschiedliche Sicherheitsanforderungen abhängig vom Ergebnis der Schutzbedarfsanalyse hat, können die Vorgaben dieses Dokuments, je nach Art der erbrachten Dienstleistung vom AG im Einvernehmen mit dem AN eingeschränkt oder auch erweitert und ergänzt werden.

1.3 Begriffsdefinition

Asset (Wert): Unter einem Asset (Wert) sind beispielsweise alle informationsverarbeitenden Einrichtungen, Betriebsmittel, Daten und Informationen zu verstehen, die für den Betrieb der wesentlichen Geschäftsprozesse notwendig sind.

IKT-System: Unter einem IKT-System ist jedes informationsverarbeitende System, IT-Komponente, Dienst oder jede informationsverarbeitende Infrastruktur zu verstehen.

Software: Unter Software ist jedenfalls folgendes zu verstehen z.B. Betriebssystem, Middleware (Datenbanksysteme, Webserver, Mailserver, etc.), standardisierte Anwendersoftware, Mobile Applikat-ionen, Individualsoftware, Sicherheitssoftware

2 Geltungsbereich

Die vorliegenden Bedingungen und Bestimmungen (Informationssicherheitsanforderungen) gelten innerhalb der Wien Energie GmbH unabhängig vom Standort für die Beschaffung von Dienstleistungen und IKT-Systemen.

3 Abkürzungen und Begriffe

Begriff / Abkürzung	Beschreibung
AG	Auftraggeber
AN	Auftragnehmer
BCM	Business Continuity Management
BDEW	Bundesverband der Energie- und Wasserwirtschaft
BIA	Business Impact Analysis
BSI	Bundesamt für Sicherheit in der Informationstechnik
CISO	Chief Information Security Officer
DSG	Datenschutzgesetz
DSGVO	Datenschutzgrundverordnung
EU-DVO	Durchsetzungsverordnung der Europäischen Union
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnik
ISB	Informationssicherheitsbeauftragter
ISO	International Organization for Standardization
ISMS	Informationssicherheits-Managementsystem
ISI	Informationssicherheit
IT	Information Technology
KRL	Konzern Richtlinie
KPI	Key Performance Indicator
NDA	Non-Disclosure Agreement
OT	Operational Technology
SCRM	Supply Chain Risk Management
SLA	Service Level Agreement
SPS	Speicherprogrammierbare Steuerung
TKG	Telekommunikationsgesetz
TLV	Technisches Leistungsverzeichnis
VPN	Virtual Private Network
WE	Wien Energie GmbH

Tabelle 1 Abkürzungen und Begriffe

1.4 Verwendete Standards

- EU-DVO 2024/2690 der Kommission vom 17. Oktober 2024
- ENISA Technical Implementation Guidance vom 26.06.2025
- ISO27001:2022
- BSI IT Grundschutz

4 Durchführungsinhalte

4.1 Betriebsmodell

4.1.1 Allgemeiner Verantwortungsbereich des AN

Generell liegt es in der Verantwortung eines AN, die durch den Auftraggeber festgelegten Anforderungen einzuhalten. Darüber hinaus muss ein AN von Produkten / Dienstleistungen die in der Industrie anerkannten Standards der Informationssicherheit und/oder andere regulatorische Standards und Vorgaben für Dienstleistungen / Produkte gewährleisten. Der AN hat die Verpflichtungserklärung bzgl. Vertraulichkeit von Informationen des AG (NDA) zur Kenntnis zu nehmen und diese vor jeglicher Art von Leistungserbringungen zu unterzeichnen. Der AG stellt diese dem AN bereit.

Zudem ist ein Eskalationsprozess zu vereinbaren, um Verstöße gegen Vereinbarungen und Informationssicherheitsfragen zu behandeln. Die Kontaktinformationen sind als Teil der Vertrags-/Projektdokumentation zwischen dem Auftraggeber und dem Auftragnehmer zu dokumentieren.

Der AN muss Sicherheitsanforderungen mit seinen Subunternehmern, die Teile der Dienstleistung erbringen oder wesentliche Bedeutung für die Erbringung der Dienstleistung haben, vereinbaren.

Die Sicherheitsanforderungen an die Subunternehmer müssen mindestens in dem vereinbarten Umfang weitergereicht bzw. definiert und schriftlich dokumentiert werden, damit der AN sicherstellen kann, dass seine Verpflichtungen gegenüber dem AG vollständig erfüllt werden. Der AN ist gegenüber dem AG für die Überwachung seiner Subunternehmer zuständig sowie für die Einhaltung der weitergereichten Anforderungen.

Es ist sicherzustellen, dass die folgenden Anforderungen bezüglich Informationssicherheit bei jeglicher Beschaffung, Errichtung oder Änderung von IKT-Systemen eingehalten werden. Die von der Wien Energie GmbH zu beschaffenden Systeme müssen den folgenden Vorgaben entsprechen:

- Für zu beschaffende oder zu errichtende IKT-Systeme ist der Schutzbedarf durch den AG in Bezug auf die Kriterien Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität (im Rahmen einer Business Impact Analyse) zu ermitteln.
- Der AN ist verpflichtet, die Verfügbarkeit in geeigneter Form (z.B. durch technische Redundanzkonzepte, Allokation personeller Ressourcen) nachzuweisen.
- Es ist sicherzustellen, dass IKT-Systeme den Anforderungen der bestehenden zentralen Informationssicherheitssysteme der Wien Energie GmbH entsprechen. Dazu zählen unter anderem Schnittstellen zu Protokollierungs- und Überwachungssystemen oder Systemen zur Erkennung von Datenverlusten.
- IKT-Systeme sind vor Inbetriebnahme mit handelsüblichen Schwachstellenscanner auf Schwachstellen zu (über-) prüfen. Wesentliche Schwachstellen sind gegebenenfalls zu beheben.
- Bei der Errichtung ist sicherzustellen, dass Benutzer (z.B. Endanwender oder Operatoren) und Betreiber über deren Pflichten und Verantwortlichkeiten im Betrieb der IKT-Systeme informiert werden.

4.1.2 Allgemeiner Verantwortungsbereich des AG (Wien Energie GmbH)

Die Vertragsbeziehung zwischen AN und AG erfolgt über ein abgestimmtes Phasenmodell (Planung inkl. Risikobewertung, Auftragsvergabe, Integration/Inbetriebnahme, Produktive Nutzung, Außerbetriebnahme

4.1.3 Rollen und Ansprechpartner

Ansprechperson Informationssicherheit: Es muss eine Ansprechperson seitens des AN geben für die Kommunikation zwischen AN und AG. Diese Person muss auskunftsberechtigt sein, aber nicht zwingend auskunftsfähig – sie kann auch relevante Informationen beim AN für den AG einholen.

Serviceverantwortlicher (Betriebsführung): Die Aufgaben und Verantwortlichkeiten von Serviceverantwortlichen des sind via SLAs zu regeln, auch in Hinblick auf etwaige Erweiterungen (Change Requests).

4.1.4 Sicherheit im Personalwesen des AN

Jeder, der im Namen des AN agiert, der entfernten oder lokalen Zugriff auf das Informationssystem des AG haben muss, muss Informationen zu seiner Identität bereitstellen. Der AN stellt sicher, dass in seinem Namen kein Zugang missbraucht wird und er die volle Verantwortung übernimmt, sollte sich herausstellen, dass dieser Fall eintritt. Sollte der AN mit Subunternehmern zusammenarbeiten, um den Vertrag mit dem AG zu erfüllen, muss der AN diesen ausdrücklich als Subunternehmer identifizieren und er muss sicherstellen, dass der Subunternehmer die gleichen Anforderungen erfüllt.

Auf Verlangen des AG ist der AN verpflichtet, nur überprüftes Sicherheitspersonal, z. B. geprüft von nationalen Behörden, zum Umgang mit sensiblem Equipment einzusetzen. Der AN muss in diesem Fall Sicherheitsüberprüfungen von Mitarbeitern, die neu in die Organisation kommen, implementiert haben. Eine Sicherheitsüberprüfung muss zumindest eine Prüfung der Identität der Person sowie eine Prüfung auf Vorstrafen beinhalten. Der AN trägt dafür Sorge, dass sein eingesetztes Personal bzw. eingesetzte Erfüllungsgehilfen entsprechend ihrem Aufgabenbereich einen Nachweis der Qualifikation für die Durchführung der beauftragten Leistung erbringen (Ausbildung, Berufserfahrung, Referenzen, Unterweisungen, etc.).

4.2 Implementierung

4.2.1 Systemdokumentation

Der AN hat eine Systemdokumentation zu übergeben, die es dem AG ermöglicht, das System entsprechend den Vorgaben der Wien Energie GmbH zu betreiben und zu warten.

Anforderungen dieses Vorgabendokuments sind an Sublieferanten durch den AN zu überbinden. Die Dokumentation muss folgende Informationen (sofern anwendbar) beinhalten: Prozesse für Regelbetrieb (d.h. Verantwortlichkeiten, Toolunterstützung je IT/OT Komponente), Betriebsverfahren sollen dokumentiert, gewartet und allen Benutzern, die sie brauchen, zur Verfügung gestellt werden, dies beinhaltet Mitwirkungspflichten des AN wie z.B. Sicherheits- und Datenschutzanforderungen aus Informationsrisikoprozess bzw. der AN verpflichtet sich für Tätigkeiten wie Schutzbedarfsfeststellungen o.ä. Informationen bereitzustellen.

4.3 Lieferantenmanagement

Der AN beschreibt die für das IKT-System des AG zusätzlich weitere relevante Lieferanten des AN inklusive deren Aufgaben und Steuerung durch den AN.

4.4 Releasemanagement

Vorgaben zur sicheren Entwicklung sind entsprechend via SLAs zwischen dem AG und AN zu regeln.

4.5 Betrieb

4.5.1 Asset Management

Dem AG ist eine Gesamtdokumentation über das Design des Gesamtsystems zur Verfügung zu stellen. Darin beschrieben sind der Aufbau des Systems, die Architektur und die Interaktion aller beteiligten Komponenten. Bei komplexen IT/OT Systemen ist dem AG eine Asset-Liste zu übergeben.

4.5.2 Availability / Capacity Management

Availability – und Capacity Management sind vertraglich via SLAs zu regeln. Die Parameter hierfür sind je nach Kontext und Kritikalität zwischen dem AN und dem AG zu vereinbaren.

4.5.3 Threat Intelligence

Der AN verpflichtet sich, dem AG Aufzeichnungen über vergangene und Pläne für zukünftige Überprüfungen technischer Schwachstellen bereitzustellen.

4.5.4 Logging

Vom AN ist ein Loggingkonzept für sicherheitsrelevante Systemzustände von IKT-Systemen und Ereignissen vorzulegen.

4.5.5 Monitoring

Vom AN ist ein Monitoringkonzept zur aktiven Überwachung des IKT-Systems vorzulegen.

Wenn möglich sind die bei der Wien Energie GmbH eingesetzten Monitoring Lösungen zu verwenden.

4.5.6 Schwachstellen – und Patchmanagement

Es ist sicherzustellen, dass zu beschaffende oder zu errichtende IKT-Systeme über deren gesamten Lebenszyklus (oder zumindest in der Vereinbarten Laufzeit) mit Updates vom Auftragnehmer oder dem Hersteller versorgt werden können. Dem AN obliegt die Technische Verantwortung für die Überprüfung und Implementierung von Updates/Upgrades, Hotfixes und Umgehungslösungen gemeinsam mit den entsprechenden Lieferanten der Software
Das gesamte System mit all seinen Komponenten, d.h. inkl. Erweiterungen und Verbesserungen muss patchfähig sein, damit bekannte Sicherheitslücken beseitigt werden können. Dies umfasst neben dem Betriebssystem und der Firmware auch Applikationen und Hilfskomponenten, die von Dritten bezogen werden. Der AN muss über einen Prozess verfügen, um Sicherheitslücken zu behandeln (z.B. Automatisierte Prüfungen von Konfigurationsparametern mittels Schwachstellenscanner, Scripts oder anderen Prüftools, etc.).

Bei Bekanntwerden sehr kritischer Sicherheitslücken ist der AN verpflichtet, zeitnah und auf seine Kosten zu überprüfen, ob sein Produkt davon betroffen ist und den AG entsprechend zu verständigen. Der AN garantiert während des gesamten Betriebszeitraums, dass entdeckte Sicherheitslücken rasch

und zeitnah auf eigene Kosten (im Rahmen bestehender Wartungsverträge) behoben werden oder zumindest bis zur endgültigen Behebung kompensierende Risikomaßnahmen anbieten.

4.5.7 Schutz vor Schadsoftware / Malware-Schutz

Der AN verpflichtet sich, seine Produkte und Dienstleistungen regelmäßig dem aktuellen Stand der Technik entsprechend frei von Malware, Spyware, verstecktem Code oder sonstigen verborgenen Hintertüren zu halten, die geeignet sind, die Informationssicherheit des Services zu kompromittieren. Der AN muss ebenfalls Endgeräte und OT-Komponenten vor Schadsoftware schützen.

Ist das IKT-System nicht mit dem bei der Wien Energie GmbH eingesetzten Malware-Schutz kompatibel, so hat der AN ein mit seinem Produkt kompatibles Virenschutzprogramm zu nennen, welches dem der Wien Energie GmbH gleichwertig ist.

4.5.8 Sichere Konfiguration / Systemhärtung

Der AN gewährleistet den Stand der Technik der Informationssicherheit in allen seinen Produkten und Dienstleistungen. Er hat den Stand der Technik bei bestehenden Wartungsverträgen in angemessenen Wartungszyklen stets anzupassen.

- Funktionsumfang und damit die Anzahl vorhandener Programme, Software-Module und Netzwerkprotokolle auf Komponenten sind auf das für den Systembetrieb nötige Minimum zu reduzieren. Alle nicht benötigten Dienste sind auf das Minimum zu reduzieren.
- vergebene Berechtigungen sind auf ein Minimum zu beschränken.
- Anmeldeversuche am System müssen protokollierbar sein.
- Default-, bzw. Initialpasswörter müssen änderbar sein.
- Es dürfen nur nach dem Stand der Technik sichere Übertragungsprotokolle verwendet werden.
- Nicht verwendete Schnittstellen sind zu deaktivieren, der AG hat die Möglichkeit dies direkt auf den Geräten des ANs zu kontrollieren. Dazu muss mind. ein User mit Passwort für den AG angelegt und bekannt gegeben werden.

4.5.9 Einsatz von kryptografischen Verfahren und Methoden

Daten sind grundsätzlich vor unerlaubter Einsichtnahme und Manipulation zu schützen (Sicherstellung der Vertraulichkeit und Integrität). Es sind grundsätzlich kryptografische Verfahren und Verschlüsselungsstandards gemäß Stand der Technik zu verwenden. Es dürfen nur anerkannte Verschlüsselungs-Verfahren und Schlüsselmindestlängen verwendet werden, die nach dem Stand der Technik als zukunftssicher gelten. Die jeweiligen Detailanforderungen sind kontextspezifisch abzuklären. Selbstentwickelte Verschlüsselungsalgorithmen sind nicht erlaubt.

4.5.10 Technologisches Change Management in Bezug auf Informationssicherheit

Es ist vom AN sicherzustellen, dass aufgrund von geänderten informationssicherheitstechnischen Anforderungen seitens der Wien Energie GmbH die Möglichkeit besteht, Anpassungen am Vertragswerk vorzunehmen bzw. diese Anforderungen an etwaig vorhandene Sublieferanten zu übertragen.

Der AN ist zu verpflichten, jegliche Änderungen an oder bei der Dienstleistungserbringung für die Wien Energie GmbH zur Kenntnis zu bringen, bspw. Änderungen an den Netzwerken, Nutzung neuer Technologien, etc.

4.5.11 Zugriffsrechte bzw. Zugriffsschutz

IKT-Systemen haben über eine Zugangssteuerung bzw. einen Zugriffsschutz zu verfügen. Es ist eine Benutzerverwaltung zu implementieren, die die Einschränkung des Zugriffs auf Daten und Informationen nach dem Need-to-Know-Prinzip erlaubt. Es sollen Mechanismen zur Benutzer-Authentifikation vorgesehen werden, auf Anforderung auch MFA. Die Benutzer-Authentifikation ist zumindest mittels Kennwörter sicherzustellen. Die Kennwörter haben den Kennwortvorgaben der Wien Energie GmbH zu entsprechen.

4.5.12 Fernzugang / Wartungszugänge

Es sind ausschließlich die von der Wien Energie GmbH zur Verfügung gestellten Fernzugänge zu verwenden.

4.5.13 Auswahl von Sublieferanten

IKT-Systeme sowie Daten und Informationen sind vor unbefugtem Zugriff durch AN zu schützen. Dazu sind folgende Inhalte zu beachten:

- Die Schnittstellen zu AN (Dienstleistern und Lieferanten) werden vom AG erhoben und verwaltet.
- Die AN müssen Mindeststandards gemäß den Vorgaben der Wien Energie GmbH einhalten.

Diese Vorgaben können je nach notwendigem Schutzbedarf die folgenden Inhalte umfassen:

- Sicherheitsprüfung des eingesetzten Personals
- Einlasskontrollen (Zutritt nur nach Anmeldung, Ausweiskontrolle, etc.)
- Akzeptanz und Unterzeichnung der Verhaltensregeln und Sicherheitsanweisungen
- Zugangskontrollen (Zugang zu Räumlichkeiten, IKT-Systeme, Daten und Informationen)
- Unterzeichnung einer Geheimhaltungserklärung und/oder Datenschutzvereinbarungen
- Vorgaben zur etwaigen Überwachung der durchzuführenden Tätigkeiten durch den AG
- Regelung zur Speicherung, Verarbeitung, Weitergabe, Übertragung und Löschung von Daten
- Unterzeichnung der Regelung zur Durchführung von Fernwartungstätigkeiten
- Vorgaben hinsichtlich Einbringung externer Hard- und Software
- Regelungen bezüglich Subauftragnehmer
- Recht auf Durchführung von Inspektionen und Audits beim Sublieferanten durch den AG oder ihren Beauftragten
- Vorgaben bezüglich Sicherheitsmanagement (z.B. Nachweis einer ISO/IEC 27001 Zertifizierung oder ähnlichen Zertifizierungen)
- Etc.

Für IKT-Systeme mit hohem oder sehr hohem Schutzbedarf bzw. IKT-Systeme der kritischen Infrastruktur gemäß NISG muss der AN sicherzustellen, dass die Mindestsicherheitsanforderungen der Wien Energie GmbH auch für etwaige Sublieferanten Geltung finden.

Für IKT-Systeme mit hohem oder sehr hohem Schutzbedarf ist zusätzlich das Whitepaper von Österreichs Energie, „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ in seiner aktuellen Version zu berücksichtigen.

4.5.14 Webapplikationen

Die Applikation ist in verschiedene Module (z.B. Präsentations-, Anwendungs-, Datenschicht) zu trennen. Gegebenenfalls sind diese Module auf verschiedene Server zu verteilen. Sämtliche Parameter, die vom Anwender (bzw. seinem Webbrowser) an die Webanwendung gesendet werden, sind genau auf Gültigkeit, maximale Länge, sowie auf korrekten Typ und Wertebereich zu prüfen.

Dies gilt auch für Parameter, die von der Web-Anwendung selbst in einem vorhergehenden Schritt zum Anwender geschickt wurden. Dabei ist insbesondere auf sog. XSS- und Injection Sicherheitslücken zu achten, über die ein Angreifer eigene Kommandos ausführen kann. Es ist besonders auf sicheres Session-Management zu achten. Die Übertragung von Session-IDs ist durch TLS-Verschlüsselung zu schützen. Session Timeouts müssen einstellbar sein.

4.5.15 Sicherheit von Anwendungsdiensten in öffentlichen Netzwerken

Informationen, die durch Anwendungsdienste über öffentliche Netzwerke übertragen werden, sind vor betrügerischer Tätigkeit, Vertragsstreitigkeiten und unbefugter Offenlegung sowie Veränderung zu schützen. Es gelten folgende Vorgaben:

- Mechanismen zur sicheren Authentifizierung der involvierten Parteien sind zu implementieren
- Die Vertraulichkeit und Integrität der Informationen sind mittels Verschlüsselung sicherzustellen.

4.5.16 Netzwerksicherheit

Folgende Anforderungen an die Netzwerksicherheit sind zu befolgen:

- Netzwerksegmente mit unterschiedlichem Schutzbedarf und Sicherheitsstufen müssen voneinander getrennt werden. Netzwerkperimeter müssen einen Firewallschutz haben. Firewallregeln müssen einen dokumentierten Freigabeprozess durchlaufen.
- Authentisierungsmerkmale (Passwörter, PINs) dürfen nur verschlüsselt über das Netzwerk übermittelt werden.
- Aus dem Internet erreichbare administrative Zugänge oder Netzwerkports für den technischen Zugriff müssen abgeschaltet oder angemessen abgesichert werden (z. B. durch 2-Faktor-Authentifierung).
- Datensicherungs- und Wiederherstellungsprozesse sind etabliert. Datenwiederherstellungstests werden regelmäßig durchgeführt.
- Sicherer physischer Transport von Speichermedien (Verschlüsselung, physische Absicherung).
- Software-Change-Prozesse für Produktivumgebungen sind etabliert und werden befolgt.
- Es muss sichergestellt werden, dass die Systeme sich nicht mit unautorisierten Access-Points verbinden können bzw. dass keine unautorisierten Netzwerke aufgebaut werden.

4.6 Wartung

Der AN ist verantwortlich für das Durchführen und Kommunizieren an den AG von:

- Informationszeitpunkte, Wartungsverteiler, Wartungsaktivitäten, Überschreitungen, Tests, Remotewartung
- Während der Wartung ist es notwendig Updates/Upgrades, Hotfixes und Umgehungslösungen zu testen, bevor sie in die Wirksysteme eingespielt und aktiv gesetzt werden.
- Wartung der installierten Betriebssysteme und Virtualisierung Software

4.7 Service- / Störungsmanagement

Der AN ist verantwortlich für die

- Identifikation, Aufnahme, Priorisierung, Auswirkung, Dringlichkeit, Kategorisierung von Störungen
- Definition von Ansprechpartnern für Diagnosen im Zuge der Ticket-Bearbeitung (Bereitstellung von Logfiles, Traces, Datadumps, etc.).
- Interne Kommunikation mit weiteren Stakeholdern

Sind Arbeiten notwendig, die außerhalb des Wartungsvertrages liegen, ist dem AG ein gesondertes Angebot vor Beginn der Arbeiten vorzulegen und in Abstimmung mit dem AG durchzuführen (z.B. für die Beschaffung eines neuen Systems ist durch den AG an den AN ein erneutes Angebot zu legen).

4.8 Informationssicherheitsvorfall Management

Prozesse zur Reaktion auf Sicherheitsvorfälle, sowie die dazugehörigen Rollen und Verantwortlichkeiten müssen nach dem Allgefahrenansatz aufgesetzt werden und sind in der zu erstellenden Dokumentation anzuführen. Grundlage für ein wirksames Informationssicherheitsvorfall Management ist wegen der möglichen weiterführenden Auswirkungen ein ausgeprägtes IT/OT-Notfallmanagement. Beide Ansätze sollten auf das unternehmerische BCM den AN aufsetzen und mit aufeinander abgestimmt sein.

Der AN ist verpflichtet, Sicherheitsvorfälle, die potentiell einen negativen Effekt auf materielle und immaterielle gelieferte oder auf dem Informationssystem gespeicherte Informations-/Vermögenswerte beim AG haben könnten, unverzüglich dem AG zu melden.

4.8.1 Eskalationsmanagement / -prozeduren

Der AN definiert mit dem AG Vorgaben und Prozeduren zum Eskalationsmanagement sowohl auf fachlicher als auch hierarchischer Ebene.

4.8.2 Meldepflichten bzgl. Informationssicherheitsvorfälle

Der AN ist verpflichtet, alle erkannten Schwachstellen oder aufgetretene Sicherheitsvorfälle unverzüglich dem AG zu melden.

*4.8.3 **Backup- und Wiederherstellungsprozess und Datensicherung***

Der AN hat ein Datensicherungskonzept, gemäß den Vorgaben der Wien Energie GmbH zu implementieren. Die Vorgaben dazu werden im entsprechenden zugehörigen Technischen Leistungsverzeichnis (TLV) definiert.

4.9 Notbetrieb und Rückführung in den Normalbetrieb

Der AN liefert dem AG eine Beschreibung der Prozesse zur Handhabung von Notfällen.

4.9.1 Wiederanlaufzeiten und Sicherheit des IT/OT-Betriebs

Der AN liefert ein Konzept zur Datensicherung, um diese z.B. nach dem Generationenprinzip in mindestens drei Generationen durchzuführen. Jahressicherungen sind mindestens acht Jahre zu archivieren. Für den Katastrophenfall ist eine Lösung zu konzipieren, zu implementieren und zumindest einmal je Kalenderjahr zu testen.

4.9.2 Personal für Notfall- und Krisenübungen

Der AN stellt ggf. Personal zur Verfügung, die an gemeinsamen Notfall- und Krisenübungen mit dem AG teilnehmen. Der Bedarf an Ressourcen wird seitens des AG rechtzeitig an den AN kommuniziert, vice versa kommuniziert der AN mindestens 4 Wochen vor einer geplanten Notfallübung Nicht-Verfügbarkeiten des Lieferantenpersonals.

4.9.3 Teilbarkeit

Die genannten Pflichten des ANs sind Hauptleistungspflichten und unteilbar, sofern die Vertragsparteien (AG und AN) nichts anderes vereinbaren.

4.10 Audit Management

Der AN räumt dem AG das Recht der Kontrolle (Audit) ein. Der AN stimmt zu, dass der AG oder ein durch ihn beauftragter Dritter den AN während der Laufzeit des Vertrages in Bezug auf dessen Informationssicherheit und Einhaltung datenschutzrechtlicher Bestimmungen auditieren darf. Basis der Audits in der Informationssicherheit ist abhängig von der Größe und Kritikalität von Systemen sowie der jeweils aktuelle Stand der Technik. Geprüft wird die angemessene Umsetzung der vereinbarten Informationssicherheitsanforderungen bezogen auf den Auftrag (Dienstleistung, Produkt) und den Aufbau und die Wirksamkeit der Informationssicherheitsorganisation beim Auftragnehmer. Basis der datenschutzrechtlichen Audits sind die DSGVO sowie das DSG.

Der AG kündigt ein anlassloses Regelaudit spätestens sechs Wochen vor dessen Durchführung an. Anlassbezogene Audits können in Abhängigkeit von der Schwere des Anlasses bzw. der Dringlichkeit auch kurzfristiger erfolgen. Der Auftragnehmer stellt rechtzeitig (i.d.R. spätestens drei Wochen vor Durchführungstermin) die benötigten Unterlagen wie z.B. Managementberichte, betriebliche Unterlagen (Konfigurations- und Berechtigungsdaten), Berichte aus dem ISMS zur Verfügung und kommt seinen Mitwirkungspflichten, z.B. Erteilung der notwendigen Zugriffsrechte, Bereitstellen von Dokumentationen und Zugängen, im Rahmen des Audits nach.

Der AG stellt dem AN die Ergebnisse des Audits in Berichtsform zur Verfügung. Der AN verpflichtet sich, die als kritisch gekennzeichneten Abweichungen zu beheben und den Fortschritt der Behebungen zu berichten. AG und AN vereinbaren Umfang und Zeitplan dieser Verbesserungsprojekte einvernehmlich. Der AG behält sich das Recht vor, den Fortschritt der Verbesserungsmaßnahmen vor Ort zu prüfen. Für die Vorbereitung dieser Prüfungen gilt der oben für Regelaudits genannte Zeitrahmen. Die beim AG anfallenden Kosten eines anlasslosen Regelaudits werden vom AG getragen. Die beim AG anfallenden Kosten eines anlassbezogenen, z.B. durch einen Sicherheitsvorfall initiierten Audits werden vom AN getragen. Soweit ein Audit nachweislich aus berufsrechtlichen Gründen nicht wie vom AG geplant durchgeführt werden kann, informiert der AN den AG zeitnah über diese Gründe. Die Parteien stimmen dann einen modifizierten Auditplan ab. Dabei werden sowohl das für den AN geltende Berufsrecht als auch die Interessen des AG berücksichtigt.

Dem AG wird das Recht der Einsichtnahme und Kontrolle des ANs bei Beschaffungsgegenständen mit hohem Schutzbedarf bzw. bei Verschlechterung der Vertrauensbeziehung zum AN, sei es auch durch ihn beauftragte Dritte, eingeräumt. Der AN verpflichtet sich, dem AG jene Informationen zur Verfügung zu stellen, die zur Kontrolle notwendig sind. Im Zuge der Kontrolle durch den AG festgestellte Mängel sind durch den AN in Absprache mit dem AG zu beheben.

4.11 Berichtswesen

Der AG kann vom AN einen Statusbericht zur Informationssicherheit der bezogenen Leistung anfordern. Dieser enthält z.B. Informationen zu Abweichungen von vereinbarten Informationssicherheits-anforderungen, Verlaufsstatistiken zu Sicherheitsvorfällen und Sicherheitspatches, Status zum Schwachstellenmanagement und Auditergebnissen, Aufwände zur Behebung von Informations-sicherheitsvorfällen und Fakturierung bei gesonderter Vereinbarung von Sicherheitsmaßnahmen.

4.12 Vorkehrungen für die Beendigung des Vertragsverhältnisses

Der AN hat im Falle der Beendigung des Vertrages, aus welchem Rechtsgrund auch immer, oder auf Verlangen die Daten des AGs, die ihm in Zusammenhang mit der Leistungserbringung zugänglich gemacht wurden, dem AG zu übergeben und bei sich unwiederbringlich zu löschen sowie das Löschen der Daten schriftlich zu bestätigen.

4.13 Außerbetriebnahme

Es dürfen keine End of Life (EoL) bzw. End of Service Geräte im Einsatz sein (solche Geräte müssen dem AG gemeldet und getauscht werden.

5 Mitgeltende Unterlagen

Dokumententitel	Link zum freigegebenen Dokument
Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme	https://www.bdew.de/media/documents/BDEW-OE-VSE-Whitepaper-3.0.pdf

Tabelle 2 Mitgeltende Unterlagen