1. Zweck

Die vorliegenden Bedingungen und Bestimmungen (Informationssicherheitsanforderungen) stehen für die erforderlichen Informationssicherheitsmassnahmen welche für Lieferanten (Auftragnehmer) von WE gelten.
Unter Lieferanten werden in diesem Dokument auch Dienstleister und Hersteller verstanden und im weiteren als Auftragnehmer (AN) bezeichnet. Der Betreiber des Systems oder der kritischen Infrastruktur wird als Auftraggeber bezeichnet (AG).
Zweck dieses Dokuments ist es, die wichtigsten Sicherheitsanforderungen an die Lieferanten von Produkten oder Dienstleistungen für WE zu identifizieren und in Form einer Vereinbarung mit den AN zu dokumentieren.
Die Vorgaben dieses Dokuments sind für alle Neuanschaffungen, Erweiterungen, bzw. Umbauten oder Adaptionen (Upgrades, etc.) oder Dienstleistungen an bestehenden IKT-Systemen und IT-Komponenten, die Daten und Informationen verarbeiten, weiterleiten, empfangen oder speichern, anzuwenden.
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.

2. Geltungsbereich (z.B. Bereich, betroffene Prozesse)

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

3. Abkürzungen und Begriffe

Begriff, Abkürzung	Bedeutung
Need-To-Know-Grundsatz	Jede IT-Komponente erhält nur die Rechte die für die für die Ausführung der Funktionen notwendig sind um die Gesamtfunktionalität zu gewährleisten. Die dabei benötigten Systemrechte sind so niedrig wie möglich anzusetzen.
Asset (Wert)	Unter einem Asset (Wert) sind beispielsweise alle informationsverarbeitende Einrichtungen, Betriebsmittel, Daten und Informationen zu verstehen, die für den Betrieb der wesentlichen Geschäftsprozesse notwendig sind.
Daten	Maschinenlesbare und bearbeitbare Repräsentation von Information. Potentielle Information.
Informationen	Daten mit Semantik. Potentiell oder aktuell vorhandenes, nutzbares oder genutztes Wissen.
IKT-System	Unter einem IKT-System ist jedes informationsverarbeitende System, IT-Komponente, Dienst oder jede informationsverarbeitende Infrastruktur zu verstehen. Unter einem IKT-System sind jedenfalls zu verstehen: • Netzwerkkomponenten (Switches, Router, Modems, WLAN Access Points, Firewall, Load Balancer, etc.) • Serversysteme, Clientsysteme, Speichersysteme, Telekommunikationsgeräte, Kommunikationsverbindungen, Anwendungen Leitsysteme, primäre und sekundäre Automatisierungs- und Fernwirktechnik (z.B. Steuerungsgeräte, SPS, Video- und Leittechnikkomponenten)
IT-Komponente	Unter IT-Komponenten werden hier generell alle Systeme mit IT-Bezug (Hardware, Software) zusammengefasst.
Integrität	Gewährleistung der Korrektheit der verarbeiteten Daten. D.h.: Richtigkeit, Vollständigkeit und Schutz gegen unbemerkte Änderungen sowie der Sicherstellung der eindeutigen Zuordenbarkeit von verarbeiteten Daten zu Personen (Authentizität) auch gegenüber Dritten (Nicht-Abstreitbarkeit).

Maßnahme	Mittel zur Veränderung von Risiken. Maßnahmen umfassen Prozesse, Richtlinien, Geräte, Methoden oder anderweitige Handlungen, die Risiken verändern.
Netzwerkdienst	Unter Netzwerkdiensten sind beispielsweise Dienste zur Bereitstellung von Verbindungen (z. B: LAN, WLAN, MPLS, Internet-Anbindungen), VPNs, Outsourcing- und Cloud Services, E-Mail, Fernwartung, etc. zu verstehen.
NISG	Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG).
USB	Universal Serial Bus: Schnittstelle an einem PC zum Anschluss von externen Geräten oder Laufwerken.
Schwachstelle	Schwäche eines Wertes oder einer Maßnahme, die durch eine oder mehrere Bedrohungen ausgenutzt werden kann.
Software	Unter Software ist jedenfalls folgendes zu verstehen: Betriebssystem Middleware (Datenbanksysteme, Webserver, Mailserver, etc.) standardisierte Anwendersoftware Mobile Applikationen Individualsoftware Sicherheitssoftware
Verfügbarkeit	Verfügbarkeit der Information zu jedem gewünschten Zeitpunkt innerhalb des vereinbarten Zeitraums.
Vertraulichkeit	Schutz von Informationen vor Kenntnisnahme und Nutzung durch unbefugte Personen.
VPN	Virtual Private Network
Telearbeit	Telearbeit bezieht sich auf alle Formen der Arbeit außerhalb der Büroräumlichkeiten.
Zugang	Die Anmeldung bzw. das Anmelden-Können an informationsverarbeitenden Einrichtungen.
Zugriff	Die Nutzung bzw. das Nutzen-Können von Daten und Informationen.
Zutritt	Das Betreten bzw. das Betreten-Können von Geländen, Gebäuden oder Räumen.

4. Durchführungsinhalte

4.1. Allgemeine Verantwortung des AN

Generell liegt es in der Verantwortung eines AN, die durch den Auftraggeber festgelegten Anforderungen einzuhalten. Darüberhinaus muss ein AN von Produkten / Dienstleistungen die in der Industrie anerkannten Standards der Informationssicherheit und/oder andere regulatorische Standards und Vorgaben für Dienstleistungen / Produkte beachten.
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 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. Der AN räumt dem AG das Recht der Kontrolle (Audit) ein.

4.1.1. Allgemeines

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

- Für zu beschaffende oder zu errichtende IKT-Systeme ist der Schutzbedarf in Bezug auf die Kriterien Verfügbarkeit, Vertraulichkeit und Integrität (im Rahmen einer Business Impact Analyse) zu ermitteln.
- Der AN muss eine Aussage zur Verfügbarkeit seines Systems machen (MTF, MTR)

- Der AG behält sich das Recht vor eine Sicherheitsüberprüfung durch eine externes Unternehmen durchzuführen.
- Es ist sicherzustellen, dass die Kompatibilität mit bestehenden IKT-Systemen gewährleistet wird.
- Es ist sicherzustellen, dass IKT-Systeme den Anforderungen zu bestehenden zentralen Informationssicherheitssystemen der WE 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) und Betreiber (z.B. der IT-Betrieb von WE) über deren Pflichten und Verantwortlichkeiten im Betrieb der IKT-Systeme informiert werden.

4.2. Systemdokumentation

- Der AN hat eine Systemdokumentation zu übergeben, die es dem AG erlaubt, das System „sicher“ zu betreiben.

4.3. Asset Liste

- 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 Systemen ist dem AG eine Asset-Liste zu übergeben.

4.4. Schnittstellenliste / Kommunikationsmatrix

- Für jedes IKT-System ist eine Kommunikationsmatrix zu erstellen. Diese hat sämtliche Kommunikationswege (Schnittstellen) zu beschreiben, die für den Betrieb notwendig sind.

4.5. Patchmanagement

- Es ist sicherzustellen, dass zu beschaffende oder zu errichtende IKT-Systeme über deren gesamten Lebenszyklus (oder zumindest 5 Jahre) mit Updates vom Auftragnehmer oder dem Hersteller versorgt werden können.
- 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 Betriebssystem und Firmware auch Applikationen und Hilfskomponenten, die von Dritten bezogen werden.
- Der AN muss über einen Prozess verfügen, um Sicherheitslücken zu behandeln.
- Bei Bekanntwerden sehr kritischer Sicherheitslücken (gemäß CVSS) ist der Hersteller verpflichtet, zeitnah und auf seine Kosten zu überprüfen, ob sein Produkt davon betroffen ist und seine Kunden 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 ein brauchbares Compensating Measure anbieten.

4.6. 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 vorhandender 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. Initialpassworte müssen änderbar sein.
- Es dürfen nur nach dem Stand der Technik sichere Übertragungsprotokolle verwendet werden.

4.7. Datensicherung

- Der AN hat ein Datensicherungskonzept, gemäß den Vorgaben von WE zu implementieren.

4.8. 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 sind Mechanismen zur Benutzer-Authentifikation vorzusehen, auf Anforderung auch MFA. Die Benutzer-Authentifikation ist zumindest mittels Kennwörtern sicherzustellen. Die Kennwörter haben den Kennwortvorgaben der WE zu entsprechen.

4.9. Fernzugang / Wartungszugänge

- Es sind ausschließlich die von WE zur Verfügung gestellten Fernzugänge zu verwenden.

4.10. Schutz vor Schadsoftware / Antivirus

- Der AN verpflichtet sich, seine Produkte und Dienstleistungen frei von Malware, Spyware, verstecktem Code oder sonstigen verborgenen Hintertüren zu halten, die geeignet sind, die Informationssicherheit des Services zu kompromittieren.
- IKT-Systeme sind vor Schadsoftware zu schützen.
- Ist das IKT System nicht mit dem bei WE eingesetzten Virenschutz kompatibel, so hat der AN ein mit seinem Produkt kompatibles Virenschutzprogramm zu nennen, welches dem von WE gleichwertig ist.

4.11. Verschlüsselung

- 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. Selbstentwickelte Verschlüsselungsalgorithmen sind nicht erlaubt.

4.12. 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 SSL-Verschlüsselung zu schützen. Session Timeouts müssen einstellbar sein.

4.13. Logging

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

4.14. Monitoring

- Vom AN ist ein Monitoringkonzept zur aktiven Überwachung des IKT Systems vorzulegen.
- Wenn möglich sind die bei WE eingesetzten Monitoring Lösungen zu verwenden.

4.15. Sicherung 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
- Sicherstellung der Vertraulichkeit und Integrität der Informationen mittels Verschlüsselung.

4.16. Auswahl von Lieferanten

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

- Die Schnittstellen zu Auftragnehmern (Dienstleistern und Lieferanten) werden vom Auftraggeber erhoben und verwaltet.
- Die AN müssen Mindeststandards gemäss den Vorgaben von WE 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 durch den AG oder ihren Beauftragten
- Meldepflichten bezüglich Sicherheitsvorfällen
- Vorgaben bezüglich Sicherheitsmanagement (z.B. Nachweis einer ISO/IEC 27001 Zertifizierung oder ähnlichen Zertifizierungen).

Für IKT-Systeme mit hohem oder sehr hohem Schutzbedarf bzw. IKT-Systeme der kritischen Infrastruktur gemäß NISG muss der AN sicherzustellen, dass die Mindestsicherheitsanforderungen von WE 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“ zu berücksichtigen.

4.17. Änderungen der informationssicherheitstechnischen Anforderungen

Es ist vom AN sicherzustellen, dass aufgrund von geänderten informationssicherheitstechnischen Anforderungen seitens WE die Möglichkeit besteht, Anpassungen am Vertragswerk vorzunehmen bzw. diese Anforderungen an etwaig vorhandene Sublieferanten zu übertragen.
Die AN sind zu verpflichtet, jegliche Änderungen an oder bei der Dienstleistungserbringung von WE zur Kenntnis zu bringen. Dazu zählen unter anderem jedenfalls

- Änderungen an den Netzwerken
- Nutzung neuer Technologien
- Einführung neuer IKT-Systeme oder neuer Versionen
- Neue Entwicklungswerkzeuge und Entwicklungsumgebungen
- Änderungen vom Standort der Leistungserbringung
- Sublieferantenwechsel

5. Mitgeltende Unterlagen

Whitepaper von Österreichs Energie „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“

https://oesterreichsenergie.at/publikationen/ueberblick/detailseite/anforderungen-an-sichere-steuerungs-und-telekommunikationssysteme