Informationssicherheits-Anforderungen Lieferanten

Die gültige (gelenkte) Version ist intern abgelegt.

Die Informationssicherheitsvorgaben sind in elektronischer Form dokumentiert. Gedruckte Ausgaben sind persönliche Arbeitsexemplare und unterliegen nicht dem Änderungsdienst.

1) Geltungsbereich und Zielsetzung

Als kommunaler Grundversorger bietet die LINZ AG und ihre Konzerngesellschaften Produkte und Dienstleitungen an, die systemerhaltenden Charakter haben und von hoher gesellschaftlicher Bedeutung sind. Dem entsprechend werden hohe Informationssicherheits-Ansprüche an die im Konzern eingesetzten Netz- und Informationssysteme gesetzt.

Auf den folgenden Seiten werden die Mindest-Informationssicherheits-Anforderungen für Lieferanten von Dienstleistungen oder Produkten definiert. Die Anforderungen sind für alle Beschaffungen, Adaptionen (z. B. Updates, Upgrades), Erweiterungen und / oder Dienstleistungen an neuen oder bestehenden Netz- und Informationssystemen oder Komponenten davon anzuwenden.

Als Lieferanten werden in diesem Dokument sowohl IT-/OT-Dienstleister als auch Software- und/oder Hardware-Lieferanten verstanden. Diese sind im Folgenden als Auftragnehmer (kurz „AN“) bezeichnet. Der Betreiber der Netz- und Informationssysteme wird als Auftraggeber (kurz „AG“) bezeichnet.

2) Allgemeine Anforderungen

Einhaltung der Anforderungen
Es wird von allen AN erwartet, dass sie die gelisteten Anforderungen vollständig erfüllen. Zudem müssen die gelisteten Anforderungen vom Lieferanten rechtlich bindend mit seinen Sub-Lieferanten vereinbart werden, sofern diese Teile der Dienstleistung erbringen oder wesentliche Bedeutung für die Erbringung der Dienstleistung haben.

Bei Abweichungen bzw. Nicht-Erfüllung von den gelisteten Anforderungen, ist dies durch den AN an den AG zu melden. Dabei sind geplante bzw. bereits getroffene risikominimierende Maßnahmen aufzulisten. Abhängig vom Ergebnis der beim AG intern durchgeführten Schutzbedarfsanalyse können Anforderungen des vorliegenden Dokuments durch den AG eingeschränkt oder erweitert werden.

Auditrecht
Der AG hat das Recht, unter Einbeziehung des AN und nach vorheriger Ankündigung, Überprüfungen durchzuführen oder von im Einzelfall dem AN vorher namhaft gemachten Prüfer*innen durchführen zu lassen, um sich von der Einhaltung der gelisteten Anforderungen in dessen Geschäftsbetrieb überzeugen zu können. Stichprobenkontrollen sind zulässig.
Der AN ermöglicht dem AG Überprüfungen durch diesen oder einer*einen von ihm beauftragte*n Prüfer*in, wirkt daran uneingeschränkt mit, erteilt Auskünfte und ist damit einverstanden, dass zum Zweck der Überprüfung der Einhaltung dieser Vereinbarung alle relevanten Aufzeichnungen, Prozesse und Systeme geprüft und auditiert werden. Der AN stellt sicher, dass der AG sich von der Einhaltung der Pflichten des AN überzeugen kann.

Der AN stellt sicher, nach dem aktuellen Stand der Technik zu arbeiten sowie bei seinen Produkten bzw. Dienstleistungen Informationssicherheits-Maßnahmen nach dem aktuellen Stand der Technik umzusetzen.

Insbesondere sind die folgenden Anforderungen sicherzustellen:

Organisation der Informationssicherheit
Der AN soll, falls vorhanden, Informationssicherheits-Zertifizierungen (z. B. nach ISO/IEC 27001) oder anderweitige Nachweise bereitstellen und den AG auch bei Änderungen / Aktualisierungen dieser informieren.

Der AN muss Informationssicherheitsmanagementprozesse in Anlehnung an anerkannte Sicherheitsstandards betreiben (z. B. nach ISO/IEC 27001). Die Prozesse sowie für

Informationssicherheits-Themen zuständige Personen müssen dokumentiert sein. Diese muss der Belegschaft bekannt sein und regelmäßig aktualisiert werden.

Dokumentation
Der AN stellt sicher, dass er jegliche Dokumentation zur Verfügung stellt, die die Nutzung der angebotenen Produkte bzw. Dienstleistungen erleichtert

Informationspflicht bei Security Incidents
Der AN ist verpflichtet, Security Incidents, die potenziell negative Auswirkung auf den AG haben können, unverzüglich an den AG per E-Mail an securityalerts@linzag.at zu melden.

Der AN stellt sicher, dass Security-Incident-Response-Prozesse sowie zugehörige Rollen und Verantwortlichkeiten etabliert sind und regelmäßige Schulungen und Übungen dazu durchgeführt werden.

Vulnerability Management & Patch Management
Der AN prüft von ihm bereitgestellte oder betreute Netz- und Informationssysteme kontinuierliche auf Schwachstellen und behebt diese. Dies betrifft sowohl Eigenkomponenten als auch Third-Party-Komponenten.
AN, die dem AG Produkte bereitstellen, informieren den AG umgehend schriftlich an informationssicherheit@linzag.at, wenn Schwachstellen bekannt werden.

Asset Management
Der AN stellt sicher, dass alle Assets identifiziert und dokumentiert sind, die einen Bezug zu Netz- und Informationssystemen des AG zum Zweck der Wartung oder Betriebszugang haben können.

Personelle Sicherheit
Der AN stellt sicher, dass alle Personen, die im Auftrag des AN agieren, entfernten oder lokalen Zugriff auf Netz- und Informationssysteme des AG haben, Informationen zu ihren Identitäten bereitstellen. Der AN stellt sicher, dass in seinem Namen keine Zugänge missbraucht werden.
Der AN beauftragt nur Personen, die über entsprechende Kenntnisse und Fähigkeiten bzgl. der vergebenen Leistung verfügen.
Der AN schult seine Mitarbeiter*innen nachweislich zu Informationssicherheits-Themen und passt die Schulungsinhalte regelmäßig an aktuelle Erkenntnisse an.
Auf Verlangen des AGs ist der AN verpflichtet, nur sicherheitsüberprüftes Personal (z. B. § 55 SPG) einzusetzen.

Systemhärtung
Der AN installiert und betreibt ausschließlich jene Systeme und Systemkomponenten, die für die Auftragserfüllung tatsächlich benötigt werden.
Alle nicht benötigten Netzwerkzugänge müssen deaktiviert sein. Zudem müssen die Systeme und Systemkomponenten entsprechend dem Stand der Technik konfiguriert sein.
Passwörter müssen in allen möglichen Fällen geändert werden können und insbesondere voreingestellte Initialpasswörter müssen geändert werden.
Der AN stellt sicher, dass seine Lösungen frei von bekannten „Backdoors“ sind.

Fernwartung
Der AN verwendet ausschließlich die durch den AG bereitgestellten Möglichkeiten zum Fernwartungszugriff auf AG-Ressourcen.

Penetration Tests
Der AN stellt sicher, dass Testverfahren beim AN die implementierten Sicherheitsmaßnahmen und -funktionen (Verschlüsselung, Zugriffskontrolle, Authentisierung etc.) explizit beinhalten.

Der AN führt Sicherheitsüberprüfungen in seinen Betriebsumgebungen durch (z. B. unabhängige Penetration Tests für die Systeme, die aus den externen bzw. nicht abgesicherten Netzen erreichbar sein sollen) und stellt die diesbezüglichen Berichte auf Anfrage zur Verfügung.

Kryptografie
Der AN stellt sicher, dass keine veralteten und als unsicher bekannte Kryptographie-Lösungen verwendet werden.

3) Zusatz-Anforderungen für IT-/OT-Dienstleister

Business Continuity Management
Der AN muss Notfallpläne für relevante Netz- und Informationssystemen des AG erstellen, dokumentieren und regelmäßig testen.

Zugriffsschutz und Berechtigungsvergabe
Der AN muss Maßnahmen zum Zugriffsschutz und zur Berechtigungsvergabe implementiert haben. Insbesondere ist sicherzustellen, dass

- Berechtigungen nach dem Least-Privilege-Prinzip vergeben werden,
- Freigabeprozesse für Berechtigungen auf Systemen und Informationen dokumentiert werden,
- Zugriffsrechte bei Austritt oder Wechsel zeitnahe gelöscht werden und
- Authentifizierungsmaßnahmen nach dem Stand der Technik gewählt werden.

Datenlöschung
Der AN stellt sicher, dass im Zuge der Datenlöschung / Vernichtung von Datenträgern Standards zur sicheren Löschung / Vernichtung eingehalten werden. Gelöschte Daten dürfen von Dritten unautorisiert nicht wiederhergestellt werden können.

Physische Sicherheit und Zutrittsschutz
Der AN muss angemessene Vorkehrungen zur physischen Sicherheit und zum Zutrittsschutz implementiert haben. Zutritt zu Bereichen mit Informationen oder Systemen müssen auf den autorisierten Personenkreis beschränkt sein.

Netzwerksicherheit und operationelle Sicherheit
Der AN stellt sicher, dass

- Netzwerksegmente mit unterschiedlichen Schutzbedarf und Sicherheitsstufen voneinander getrennt werden (z. B. durch Firewalls) und Firewall-Regeln einen dokumentierten Freigabeprozess durchlaufen.
- Authentifizierungsmerkmale (Passwörter, PINs etc.) nur verschlüsselt über das Netzwerk übermittelt werden.
- aus dem Internet erreichbare administrative Zugänge oder Netzwerk-Ports für den technischen Zugriff abgeschaltet oder angemessen abgesichert (z. B. durch Multi-Faktor-Authentifizierung) werden.
- Netzwerkverbindungen, Systemzugriffe und administrative Tätigkeiten zur Nachvollziehbarkeit von Angriffen oder Fehlbedienung protokolliert werden. Der AN muss sicherstellen, dass auf Alarmierungen angemessen reagiert und diese behandelt werden.
- ein angemessener Malwareschutz implementiert und aktuell ist.
- Datensicherungs- und Wiederherstellungsprozesse etabliert sind und Datenwiederherstellungstests regelmäßig durchgeführt werden.
- Change-Prozesse für (zumindest) Produktivumgebungen etabliert sind.