Zusätzliche Vertragsbedingungen – KRITIS

1. Allgemeines, Zweck und Geltungsbereich

Dieses Dokument beschreibt die zusätzlichen Bedingungen der **Leipziger Wasserwerke (LWW)** an die Informationssicherheit für vertraglich gebundene **KRITIS-relevante** Lieferanten und Dienstleister, nachfolgend **Auftragnehmer (AN)** genannt. Die zusätzlichen Vertragsbedingungen – KRITIS spezifizieren die zusätzlichen Vertragsbedingungen – Informationssicherheit.

1.1 Lieferanten- und Dienstleisterbeziehungen (KRITIS)

Durch die Tatsache, dass die LWW als Trinkwasserver- und Abwasserentsorgungsunternehmen ein kritische Infrastrukturen betreibt, gelten besondere Sicherheitsanforderungen an kritische Infrastrukturen und Standorte. Die bei kritischen Prozessen involvierten **AN** haben die nachfolgenden Regelungen konsequent einzuhalten.

1.2 Allgemeine Verantwortung des AN

Grundsätzlich gelten die Zusätzlichen Vertragsbedingungen - Informationssicherheit und KRITIS der LWW. Darüber hinaus hat der **AN** bei Produkten und Dienstleistungen für Kritische Infrastrukturen die in der Industrie anerkannten Standards der Informationssicherheit und/oder andere regulatorische Standards und Vorgaben für Dienstleistungen/Produkte zu beachten. Weiterhin gilt:

a. Ein Ausschluss von in diesem Dokument beschriebenen Anforderungen ist nur mit Begründung und schriftlicher Bestätigung der LWW zulässig.

b. Sollte der **AN** Mindestsicherheitsanforderungen nach Stand der Technik nicht einhalten können (fehlende oder abgelaufene Zertifizierung) ist dies der LWW unverzüglich anzuzeigen bzw. vor dem Ersteinsatz die Genehmigung der LWW erforderlich.

c. Auf Verlangen weist der **AN** die Herkunft kritischer Komponenten nach. Kritische Komponenten sind solche im Sinne von § 2 Abs. 13 BSIG[1] und solche, deren Ausfall oder Fehlen eine Erhöhung des Informationssicherheitsrisikos zur Folge hat. Der **AN** unterstützt die LWW bei einer entsprechenden Überprüfung der Lieferkette.

d. Gesetzlich geforderte Sicherheitszertifikate (Garantieerklärung im Sinne von § 9b Abs. 3 Satz 1 BSIG) für den Einsatz von kritischen Komponenten[1] (§ 2 Abs. 13 BSIG) in Umgebungen der kritischen Infrastruktur bei den LWW sind vom **AN**, für die gesamte Lieferkette, vorzulegen.

e. Die LWW sind gesetzlich verpflichtet den **erstmaligen** geplanten Einsatz/Einbau kritischer Komponenten[1] (§ 2 Abs. 13 BSIG) in Umgebungen der kritischen Infrastruktur bei den LWW der entsprechenden Bundesbehörde anzuzeigen. Für den Fall, dass das zuständige Bundesministerium den Einsatz der kritischen Komponente[1] nach § 9b Abs. 2 BSIG untersagt oder entsprechende Anordnungen erlässt, steht der LWW ein Rücktrittsrecht im Sinne von § 346 Abs. 1 BGB zu.

2. Management von Sicherheitsvorfällen/Business Continuity (Aufrechterhaltung der Geschäftstätigkeit)

Der **AN** wird in die Meldekette des etablierten Managementprozesses von Sicherheitsvorfällen der LWW integriert. Das bedeutet für den **AN** die Beachtung und Einhaltung n. g. Punkte:

a. Dem **AN** obliegt die Verpflichtung, sich zu Beginn der Leistungserbringung in die Meldewege für Sicherheitsvorfälle sowie die Erkennung von potenziell sicherheitsrelevanten Ereignissen der LWW einweisen zu lassen. Dazu werden dem AN durch die LWW Unterlagen, z.B. Security-Merkkarten oder Anhang 3 der ZVB Informationssicherheit, zur Verfügung gestellt.
b. Der **AN** hat sicher zu stellen, dass im Falle von eingebundenen **SUB**-Unternehmen die Meldekette der LWW berücksichtigt und nicht unterbrochen wird.

c. Wenn dem **AN** Sicherheitsereignisse oder Sicherheitsvorfälle mit Bezug zum vertraglich genannten Projekt/zur vereinbarten Dienstleitung bekannt werden, sind diese unverzüglich der LWW anzuzeigen und diese ggf. bei der Aufklärung zu unterstützen **(°)**.

d. Der **AN** benennt einen Ansprechpartner für Sicherheitsvorfälle, um eine angemessene Reaktionszeit im Gefahrenfall sicher zu stellen.

e. Je nach Signifikanz der kritischen Dienstleistung wird der **AN** ggf. in das Krisen- und Notfallmanagement der LWW eingebunden. Hierzu wird er von der LWW informiert und hat verpflichtend mit zu wirken. Ihm obliegt in diesem Fall die Verpflichtung zu erläutern, wie er im Rahmen eines Notfalls den Betrieb der Dienstleistung bzw. die Funktionsfähigkeit des Produktes so lange wie möglich aufrechterhalten bzw. so schnell wie möglich wieder in den Regelbetrieb zurückführen kann.

3. Technisches Schwachstellenmanagement

Der **AN** verpflichtet sich, in das bestehende Schwachstellen- und Patch-Management der LWW eingebunden zu werden und erteilt mit Leistungsbeginn seine Zustimmung oder verpflichtet sich sein eigenes Schwachstellen- und Patch-Management auf die eingesetzten Produkte umzusetzen und auf Anforderung nachzuweisen. Dies betrifft insbesondere:

a. Jede veröffentlichte und erkannte Schwachstelle der bereitgestellten Dienstleistung bzw. des/der Produkte/s muss vom **AN** unverzüglich an die LWW gemeldet und gemäß vertraglicher Vereinbarung geschlossen werden.

b. Der **AN** ist verpflichtet, zur Behandlung veröffentlichter und erkannter Schwachstellen, behandelnde Maßnahmen (z. B. Patche, Workarounds oder vergleichbare Maßnahmen) bereitzustellen. Basierend auf der Kritikalitätseinstufung (z. B. CVSS-Score oder BSI CSW Einstufung) sind Reaktionszeiten zur Behebung der Schwachstelle angemessen zu priorisieren/anzupassen.

c. Der **AN** ist verpflichtet, sein Produkt/Dienstleistung mit aktuellen Security-Patches zu versorgen sowie diese, nach Freigabe durch die LWW, auf aktuellem Security-Patchstand zu halten.

d. Der **AN** ist verpflichtet, zusätzlich zu seinem eingesetzten Produkt/ Dienstleistung auch die verwendeten Softwarekomponenten von Drittanbietern mit aktuellen Security-Patches zu versorgen sowie diese, nach Freigabe durch die LWW, auf aktuellem Security-Patchstand zu halten.

e. Der **AN** ist verpflichtet, den end-of-support[2] (EoS bzw. end-of-support, insbesondere security) Zeitraum und den garantierten Patchzeitraum seines Produktes/seiner Dienstleistung der LWW anzuzeigen **(*)**.

f. Der **AN** ist verpflichtet, zu jedem Update und Patch detaillierte Informationen über die Betroffenheit, Art und Auswirkungen der Änderungen zur Verfügung zu stellen.

g. Der **AN** hat alle Systeme vor Abnahme gepatcht und aktualisiert zu übergeben. Der **AN** muss die aktuellsten produktiv verfügbaren bzw. die mit der LWW vereinbarten Patchstände und Aktualisierungen einspielen.

h. Der **AN** ist verpflichtet, regelmäßige Prüfungen verwendeter Protokolle und Bibliotheken vorzunehmen. Sollten diese veraltet sein oder nicht mehr dem Stand der Technik entsprechen, sind diese zu aktualisieren bzw. anzuheben.

i. Der **AN** verpflichtet sich den Katalog bekannter ausgenutzter Sicherheitslücken bzw. Schwachstellen (https://www.cisa.gov/known-exploited-vulnerabilities-catalog) der CISA (Cybersecurity & Infrastructure Security Agency) und aktuelle Sicherheitshinweise vom Warn- und Informationsdienst (cert-https://wid.cert-bund.de/portal/wid/kurzinformationenbund.de) des BSI (Bundesamtes für Sicherheit in der Informationstechnik) regelmäßig zu prüfen und ihn betreffende Schwachstellen unverzüglich zu behandeln/ mitigieren. Systeme oder Komponenten mit einer bekannten ausgenutzten Schwachstelle dürfen nicht in Kritis-Umgebungen eingesetzt werden. Dies gilt bis die bekannte ausgenutzte Schwachstelle (z.B. gepatcht, Alternative) beseitigt wurde.

j. Die in Kapitel 3 definierten Sicherheitsanforderungen gelten auch bei smarten Feldgeräten (z.B. smarte Sensoren oder Actoren).

k. Schnittstelle, die NICHT für die Prozessdaten- und Steuerungsdatenverarbeitung notwendig sind, sind standardmäßig zu deaktivieren und nur nach Freigabe durch die LWW zu aktivieren.

4. Change-Management

Der **AN** wird in das bestehende Change- und Projektmanagement der LWW eingebunden und erteilt mit Leistungsbeginn seine Zustimmung oder verpflichtet sich sein eigenes Change- und Projektmanagement auf die eingesetzten Produkte umzusetzen und auf Anforderung nachzuweisen. Dies betrifft insbesondere:

a. Alle Systeme und/oder Komponenten, in die der jeweilige **AN** involviert ist bzw. die Vertragsgegenstand sind.

b. Alle für den funktionstüchtigen Betrieb der Systeme und Anwendungen vom Hersteller/ Dienstleister verwendeten Softwarekomponenten von Drittanbietern (z.B. Datenbanken, Webserver, Schnittstellen, Laufzeitumgebungen etc.) der Systeme oder Anwendungen.

c. Alle benötigten Zugänge und Nutzerkonten (personalisiert).

d. Die Ablauffrist (Gültigkeitsbeschränkungen) von Zugängen/Nutzerkonten (bei befristeten Projekten).

e. Jegliche Änderungen an Systemen/Diensten/Komponenten/ Softwarekomponenten von Drittanbietern und Zugängen/Nutzerkonten (Erstellung, Rechtevergabe, Deaktivierung, Neuvergabe etc.) sowie ggf. roll-back der Änderungen.

f. Freigabe und Kontrolle der Änderungen unter Vorgaben des LWW Change-Managements.

5. Softwareentwicklungen

Der **AN** ist verpflichtet, die Sicherheitsbedingungen für die sichere Softwareentwicklung einzuhalten:

a. Die Informationssicherheit ist in allen Entwicklungsphasen zu berücksichtigen (inkl. Qualitätskontrolle und Tests).

b. Neue Systeme sind entsprechend den Sicherheitsanforderungen der LWW auszuliefern.

c. Die Festlegungen der technischen Richtlinie zur Softwarestrukturierung für Automatisierungssysteme, des Technischen Regelwerkes E- & MSR-Technik sowie der Materialstandardisierung und -Vorzugsliste E- & MSR Technik sind einzuhalten.

d. Testverfahren und -fälle implementierter Sicherheitsmechanismen, beispielsweise Verschlüsselung, Zugriffskontrolle, Authentisierung etc., sind bei Bedarf mit der LWW abzustimmen.

d. Die LWW können Nachweise über die Einhaltung dieser Maßnahmen einfordern.

e. Der **AN** stellt sicherheitstechnische Informationen, beispielsweise Secure-Code-Reviews, Penetrationstest etc., bei Bedarf zur Verfügung. Dies bezieht sich nur auf finale und produktive Produkte.

f. Der **AN** stellt sicher, dass bei der Softwareentwicklung verwendete Softwarekomponenten von Drittanbietern ebenfalls die Vorgaben der sicheren Softwareentwicklung (a-e) einhalten.

6. Umgang mit Informationen, Informationsaustausch,-übertragung und -bereitstellung

a. Der Betrieb und die Nutzung von Cloudapplikationen und -services ist in kritischen Infrastrukturen der LWW verboten.

b. Der Betrieb und die Nutzung von Feldgeräten oder -Komponenten (z.B. Sensoren und Aktoren), die nicht im internen Produktionsnetzwerksegment angebunden sind und einer externen Kommunikationsanbindungen bedürfen, müssen über den privaten APN der LWW angebunden werden. Ausnahmen vom Standard bedürfen eine Risikoanalyse und sind von der LWW zu genehmigen.

*** = it.wasserwerke@L.de** oder **0341/9693666**
° = it.wasserwerke@L.de oder **0341/9693666** oder **LWW Intranet/ Self Sevice Portal/ Informationssicherheitsvorfall melden (Schloss-Symbol)**

Abkürzung:
IT = Informationstechnik (Information Technology)
OT = Operative Technologien (Operational Technology)
CISA = Cybersecurity & Infrastructure Security Agency
BSI = Bundesamtes für Sicherheit in der Informationstechnik
APN = Access Point Name (APN, auch „Zugangspunkt“)

Definition:
[1] = Kritische Komponenten im Sinne von § 2 Abs. 13 BSIG sind IT-Produkte: (Stand: März‘ 2022)
1.) die in Kritischen Infrastrukturen eingesetzt werden,
2. bei denen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können und
3.) die auf Grund eines Gesetzes unter Verweis auf diese Vorschrift
a) als kritische Komponente bestimmt werden oder
b) eine auf Grund eines Gesetzes als kritisch bestimmte Funktion realisieren.
Werden für einen der in Absatz 10 Satz 1 Nummer 1 genannten Sektoren keine kritischen Komponenten und keine kritischen Funktionen, aus denen kritische Komponenten abgeleitet werden können, auf Grund eines Gesetzes unter Verweis auf diese Vorschrift bestimmt, gibt es in diesem Sektor keine kritischen Komponenten im Sinne dieses Gesetzes
[2] = „**End of Support“ (EoS)** werden Systeme bezeichnet, bei denen keine sicherheitskritischen Fehler und Schwachstellen mehr behoben werden.