Zusätzliche Vertragsbedingungen – Informationssicherheit

Leipziger Wasserwerke

1. Allgemeines

1.1 Der Auftragnehmer (AN) benennt vor Beginn seiner Tätigkeit schriftlich einen **Verantwortlichen**, der die Einhaltung und Durchsetzung der vertraglichen Anforderungen überprüft oder veranlasst. Er muss insbesondere die nachfolgenden Informationssicherheitsanforderungen überwachen und bei Mängeln geeignete Gegenmaßnahmen ergreifen. Alle AN, die Zutritt zu Standorten der Leipziger Wasserwerke (LWW), beziehungsweise Zugriff auf LWW Informationen haben sind zur Verschwiegenheit verpflichtet.

1.2 Dem AN obliegt die Verpflichtung sich, zu Beginn der Leistungserbringung, in die **internen Meldewege** der LWW einweisen zu lassen. Dieser Verantwortliche hat nach der Einweisung dafür zu sorgen, dass alle auftretenden Informationssicherheitsvorfälle, entsprechend der Meldewege, gemeldet werden.

1.3 Der AN meldet den LWW **Abweichungen** von den vereinbarten Lieferantenprozessen und Maßnahmen im Zusammenhang mit dem Vertrag. Die LWW sind berechtigt, in regelmäßigen Abständen diese Lieferantenprozesse und Maßnahmen zu überprüfen. Um **Audits** durchzuführen, gewährt der AN Zutritt zu seinen relevanten Unternehmensteilen.

1.4 Liefert der AN Technologie-Produkte, verpflichtet er auch alle Lieferanten der Lieferkette auf die vereinbarten **Sicherheitsanforderungen** und -praktiken. Das Gleiche gilt für Leistungen einschließlich des Einsatzes von Subunternehmern in der Leistungserbringung.

1.5 Auf Verlangen weist der Auftragnehmer die **Herkunft** kritischer Komponenten nach. Als kritische Komponenten sind jene anzusehen, deren Ausfall oder Fehlen eine Erhöhung des Informationssicherheitsrisikos zur Folge haben. Der AN unterstützt den Auftraggeber bei einer entsprechenden Überprüfung der Lieferkette.

1.6 Sofern der **Lebenszyklus** von Komponenten der Informations- und Kommunikationstechnologie in Kürze endet oder diese generell nicht mehr zur Verfügung stehen werden, wird der AN die LWW über die daraus entstehenden Risiken informieren.

2. Physische Sicherheit

2.1 Anwendbare **Hausordnungen** sind einzuhalten.

2.2 Mitarbeiter des ANs und seiner Subunternehmer haben zu Räumen und Einrichtungen der LWW nur **Zutritt**, soweit sie für diese ausdrücklich autorisiert wurden. Sie tragen auf den Betriebsgeländen der LWW **Besucherausweise**.

2.3 Der physische Zutritt bei kritischen Standorten ist grundsätzlich auf vereinbarte Zonen beschränkt. Der AN muss eine aktuelle Liste des Personals mit Zutrittsberechtigung in Koordination mit den jeweiligen Standortverantwortlichen der LWW pflegen und vorhalten. Hierfür eigens ausgestellte Ausweise/Zugangskarten sind personalisiert und nicht übertragbar.

3. IT-Zugang und IT-Zugriff

3.1 Zugänge und Zugriffe innerhalb des internen Netzwerkes werden durch die LWW berechtigt und **protokolliert**.

3.2 Jeder Mitarbeiter des AN oder seiner Subunternehmer hat eine eigene Anmeldung zu nutzen. Für die Anmeldung sind sichere Passwörter zu verwenden (mindestens 10 Zeichen unter Verwendung von Groß- und Kleinbuchstaben, Zahlen). Diese Passwörter dürfen nicht weitergegeben werden.

3.3 Soweit ein Mitarbeiter des AN aktive Sitzungen (z.B. Cloud-Anwendungen, Netzwerkdienste und Anwendungen) nicht mehr benötigt, meldet er diese unverzüglich ab.

3.4 Computer, Terminals und mobile Endgeräte sind bei Nichtnutzung und Verlassen mit einem Passwort zu sperren.

3.5 Die außerhalb der beauftragten Leistung liegende Nutzung der bereitgestellten Infrastruktur sowie das Überwinden von Schutzmaßnahmen sind untersagt.

3.6 Überlassene Arbeitsmittel müssen nach Beendigung der Dienstleistung zurückgegeben werden.

3.7 Durch den AN erstellte oder bearbeitete Dokumente sind als vertraulich zu klassifizieren und auch so zu kennzeichnen.

4. Hard- und Software

4.1 Im internen IT-Netz der LWW dürfen nur vom Auftraggeber genehmigte IT-Komponenten installiert und eingesetzt werden.

4.2 Änderungen an sicherheitsrelevanten Einstellungen (Schadsoftwareschutz, Firewall etc.) sind allein der LWW vorbehalten. Insbesondere das Deaktivieren dieser Applikationen oder das Abschalten automatischer Updates ist zu unterlassen.

4.3 Fernzugriffe auf die Infrastruktur der LWW per VPN-Einwahl sind dem AN nur unter folgenden Maßgaben gestattet:

a. Einwahl nur bei Bedarf und in Abstimmung mit den LWW. Die LWW behalten sich vor, dem AN die Verwendung von Kryptographie-Lösungen vorzuschreiben.
b. Die VPN-Verbindung muss nach dem Stand der Technik gesichert sein.
c. Das zur Einwahl genutzte System muss durch aktuellen Schadsoftwareschutz geschützt sein.
d. Das zur Einwahl genutzte System muss über den aktuellsten Patch-Stand verfügen.

4.4 Es sind die vorhandenen Standards der sicheren Softwarearchitektur bei der Softwareentwicklung anzuwenden. Dabei ist der Softwareentwicklungsprozess gemäß des *Security by Design* Prinzips auszulegen.

4.5 Die Nutzung von Wechselmedien (z.B. USB-Stick, externe Festplatte, SD-Karte) ist untersagt. Ausnahmen erteilt der IT-Bereich des Auftraggebers durch ausdrückliche Einwilligung.

5. Dokumentation

5.1 Der AN hat alle Assets in seinem Informationssystem zu identifizieren und zu dokumentieren, die einen Bezug zum Informationssystem der LWW zwecks Wartung oder Betriebszugang haben können. Er hat den Schutz dieser Information angemessen sicherzustellen und zu dokumentieren.