Allgemeine Einkaufsbedingungen der Leipziger Gruppe (2024) (Leipziger AEB 2024)

Modul F. Informationssicherheit

F.1. Allgemeines

F.1.1. Der Auftragnehmer benennt vor Beginn seiner Tätigkeit schriftlich einen **Verantwortlichen für Informationssicherheit**, der die Einhaltung und Durchsetzung der vertraglichen Anforderungen überprüft oder veranlasst. Er muss insbesondere die nachfolgenden Informationssicherheitsanforderungen überwachen und bei Mängeln geeignete Gegenmaßnahmen ergreifen. Wird ein Verantwortlicher nicht ausdrücklich benannt, gelten die Vertragsunterzeichner als solche.

F.1.2. Der Auftragnehmer **meldet** dem Auftraggeber alle in Verbindung mit der Leistungserbringung auftretenden **Informationssicherheitsvorfälle** per Email, in dringenden Fällen zusätzlich telefonisch. Der Auftraggeber kann hierfür eine besondere Email-Adresse und Telefonnummer benennen. Zu meldende Vorfälle sind insbesondere die Offenlegung oder der Verlust von vertraulichen Informationen oder Geräten sowie die Kompromittierung von IT-Systemen.

F.1.3. Der Auftragnehmer meldet dem Auftraggeber **Abweichungen** von den vereinbarten Lieferantenprozessen und Maßnahmen im Zusammenhang mit dem Vertrag (z.B. Outsourcing oder Technologiewechsel).

F.1.4. Der Auftraggeber ist berechtigt, in regelmäßigen Abständen die Lieferantenprozesse und Maßnahmen im Zusammenhang mit dem Vertrag zu überprüfen. Um **Audits** durchzuführen, gewährt der Auftragnehmer Zutritt zu seinen relevanten Unternehmensteilen. Werden im Audit Feststellungen mit Sicherheitsrelevanz getroffen, müssen diese ´vom Auftragnehmer abgestellt werden.

F.1.5. Durch den Auftraggeber erstellte oder bearbeitete Dokumente sind als vertraulich zu klassifizieren und auch so zu kennzeichnen.

F.2. Zutritt

F.2.1. Anwendbare **Hausordnungen** sind einzuhalten.

F.2.2. Mitarbeiter des Auftragnehmers und seiner Subunternehmer haben zu Räumen und Einrichtungen des Auftraggebers nur **Zutritt**, soweit sie für diese vom Auftraggeber ausdrücklich autorisiert wurden. Sie tragen auf den Betriebsgeländen des Auftraggebers **Besucherausweise**.

F.2.3. **Türen** sind, wenn keine Personen anwesend sind, zu verschließen.

F.3. IT-Zugänge für Netzwerke und Systeme des Auftraggebers

F.3.1. Zugänge und Zugriffe innerhalb des internen Netzwerkes werden durch den Auftraggeber **protokolliert**.

F.3.2. Jeder Mitarbeiter des Auftragnehmers oder seiner Subunternehmer hat eine eigene Anmeldung zu nutzen. Für die Anmeldung sind sichere Passwörter zu verwenden (mindestens 8 Zeichen unter Verwendung von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen). Diese Passwörter dürfen nicht weitergegeben werden.

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

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

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

F.3.6. Überlassene Arbeitsmittel müssen nach Beendigung der Dienstleistung zurückgegeben werden.

F.3.7. Im internen IT-Netz des Auftraggebers dürfen nur vom Auftraggeber genehmigte IT-Komponenten installiert und eingesetzt werden.

F.3.8. Änderungen an sicherheitsrelevanten Einstellungen (Schadsoftwareschutz, Firewall etc.) sind allein dem Auftraggeber vorbehalten. Insbesondere das Deaktivieren dieser Applikationen oder das Abschalten automatischer Updates ist zu unterlassen.

F.3.9. Die Nutzung von Wechselmedien (z.B. USB-Stick, externe Festplatte, SD-Karte) ist untersagt. Ausnahmen erteilt der IT-Bereich des Auftraggebers durch ausdrückliche Einwilligung.

F.3.10. Fernzugriffe auf die Infrastruktur des Auftraggebers per VPN-Einwahl sind dem Auftragnehmer nur unter folgenden Maßgaben gestattet:

a. Einwahl nur bei Bedarf und in Abstimmung mit dem Auftraggeber.
b. 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.

F.4. IT-Dienstleistungen und IT-Produkte

F.4.1. Der Auftragnehmer verpflichtet alle Subunternehmer und Lieferanten der Lieferkette auf die vereinbarten **Sicherheitsanforderungen** und -praktiken.

F.4.2. Es sind branchenübliche Standards und Best Practices der sicheren System- und Softwareentwicklung sowie des sicheren IT-Betriebs anzuwenden (z.B. BSI-IT-Grundschutz, ISO 27001)

F.4.3. Auf Verlangen weist der Auftragnehmer die **Herkunft** kritischer Komponenten nach. Als kritische Komponen-

ten sind jene anzusehen, deren Ausfall oder Fehlen eine Erhöhung des Informationssicherheitsrisikos zur Folge hat. Der Auftragnehmer unterstützt den Auftraggeber bei einer entsprechenden Überprüfung der Lieferkette.

F.4.4. Ist dem Auftragnehmer bekannt, dass der **Lebenszyklus** von Komponenten der Informations- und Kommunikationstechnologie endet oder diese generell nicht mehr zur Verfügung stehen werden, wird er den Auftraggeber unverzüglich über die daraus entstehenden Risiken informieren.

F.4.5. Auf Anfrage stellt der Auftragnehmer alle Informationen zur Verfügung, die für die Bewertung der Einhaltung von vereinbarten Dienstleistungsqualitäten notwendig sind (z.B. Verfügbarkeitsberichte).