Allgemeine Einkaufsbedingungen der Stadtwerke Leipzig GmbH (2018)

Leipziger Stadtwerke

Modul F Informationssicherheit

F.1. Allgemeines

F.1.1. Der Auftragnehmer 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.

F.1.2. Der Auftragnehmer benennt zudem einen Verantwortlichen, den der Auftraggeber zu Beginn der Leistungserbringung in seine **internen Meldewege** einweist. Dieser Verantwortliche hat nach der Einweisung dafür zu sorgen, dass alle auftretenden Informationssicherheitsvorfälle entsprechend der Meldewege gemeldet werden.

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

F.1.4. Liefert der Auftragnehmer Technologie-Produkte, verpflichtet er auch alle Lieferanten der Lieferkette auf die vereinbarten **Sicherheitsanforderungen** und -praktiken.

F.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 hat. Der Auftragnehmer unterstützt den Auftraggeber bei einer entsprechenden Überprüfung der Lieferkette.

F.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 Auftragnehmer den Auftragnehmer über die daraus entstehenden Risiken informieren.

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-Zugang und IT-Zugriff

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 ist untersagt.

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

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

F.4. Hard- und Software

F.4.1. Im internen IT-Netz des Auftraggebers dürfen nur vom Auftraggeber genehmigte IT-Komponenten installiert und eingesetzt werden.

F.4.2. 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.4.3. Fernzugriffe auf die Infrastruktur des Auftraggebers per VPN-Einwahl sind dem Auftragnehmer nur unter folgenden Maßgaben gestattet:

- Einwahl nur bei Bedarf und in Abstimmung mit dem Auftraggeber.
- VPN-Verbindung muss nach dem Stand der Technik gesichert sein.
- Das zur Einwahl genutzte System muss durch aktuellen Schadsoftwareschutz geschützt sein.
- Das zur Einwahl genutzte System muss über den aktuellsten Patch-Stand verfügen.

F.4.4. Die Nutzung von Wechselmedien (z.B. USB-Stick, externe Festplatte, SD-Karte) ist untersagt. Ausnahmen erteilt der IT-Bereich des Auftraggebers durch ausdrückliche Einwilligung.