

1. Einleitung

Das Dokument dient dem Auftraggeber zum Nachweis der Einhaltung der gesetzlichen und regulatorischen Anforderungen. Der Auftragnehmer verpflichtet sich zur Einhaltung der gesetzlichen und regulatorischen Anforderungen u.a.:

- Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)
- Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz - EnWG)
- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)

2. Konkrete Anforderungen an den Dienstleister

Nachfolgend werden die konkreten Anforderungen an den Dienstleister dargelegt. Der Dienstleister wird verpflichtet die Anforderungen an die eingesetzten Subunternehmer weiterzugeben und vertraglich für die Einhaltung zu sorgen. Der Auftragnehmer gewährleistet die wirksame Umsetzung von technischen und organisatorischen Maßnahmen entsprechend dem Stand der Technik.

2.1. Nennen eines Ansprechpartners

Der Dienstleister benennt gegenüber dem Auftraggeber einen Ansprechpartner für die Informationssicherheit, der auf Anfrage an Werktagen zu den üblichen Geschäftszeiten unverzüglich Auskunft über Maßnahmen zur Einhaltung dieser Anforderungen geben kann.

2.2. Vertraulichkeit/Weitergabe

Der Dienstleister hat alle Informationswerte, die ihm vom Auftraggeber zur Verfügung gestellt werden, von denen er Kenntnis erlangt oder er für den Auftraggeber erstellt, mindestens vertraulich zu behandeln. Dies gilt unabhängig davon, ob die Informationen gekennzeichnet sind. Die Pflicht zur vertraulichen Behandlung erstreckt sich nicht oder nicht mehr auf Informationen, die nachweislich dem Empfangenden bereits vor Beginn der Zusammenarbeit bekannt waren; von einem Dritten rechtmäßig an den Empfangenden weitergegeben wurden; allgemein bekannt sind oder allgemein bekannt werden und vom Empfangenden im Rahmen eigener unabhängiger Entwicklungen erarbeitet wurden. Der Dienstleister darf Informationen offenbaren, soweit er hierzu gesetzlich oder behördlich verpflichtet ist.

Informationswerte sind nach Zweckerreichung oder früher nach Aufforderungen des Auftraggebers zurückzugeben, zu löschen oder zu vernichten. Das Protokoll der Vernichtung ist vorzulegen oder die Löschung schriftlich zu bestätigen.

2.3. Sicherer Datenaustausch

Informationswerte sind über verschlüsselte Kanäle auszutauschen.

2.4. Informationssicherheitsereignisse

Der Dienstleister hat Informationssicherheitsereignisse, die im Zusammenhang mit seiner Dienstleistung für den Auftraggeber stehen, unverzüglich an vorfall@wvv.de zu melden und entsprechende Abhilfemaßnahmen einzuleiten.

2.5. Zutrittskontrollen und Sicherheitszonen

Grundsätzlich hat sich der Dienstleister an das Besuchermanagement und dem Objektschutz des Auftraggebers zu halten.

2.6. Privilegierte Zugangs- und Zugriffsrechte auf IT-Systeme

Sofern von der Dienstleistung ein Zugriff auf die IT-Systeme umfasst ist, sind nachfolgende Regelungen einzuhalten.

2.6.1 Administrationsrechte

Sind zur Erfüllung des Auftrags durch den Dienstleister Administrationsrechte auf dem System des Auftraggebers notwendig, müssen diese beantragt, begründet und der benötigte Zeitraum benannt werden. Der Dienstleister hat anzuzeigen, wenn die Rechte nicht mehr benötigt werden. Administrationsrechte sind personengebunden und dürfen ausschließlich von der berechtigten Person zur Erbringung der vertraglichen Leistung genutzt werden. Passwörter dürfen nur der berechtigten Person bekannt sein.

2.6.2 Betrieb von Soft- und Hardware an IT-Systemen

Dem Dienstleister ist untersagt nicht explizit freigegebene Soft- und Hardware mit IT-Systemen oder Anwendungen des Auftraggebers oder dessen verbundener Unternehmen auszuführen oder zu verbinden.

Ist der Betrieb von Soft- oder Hardware für die Erfüllung des Auftrages notwendig, ist zuvor eine Genehmigung bei der jeweils verantwortlichen Führungskraft des Auftraggebers einzuholen und zu begründen.

2.6.3 Konfiguration und Wartung

Soweit der Dienstleister IT-Systeme, Anwendungen oder Komponenten des Auftraggebers konfiguriert, wartet oder parametrisiert, hat er sicherzustellen, dass der Datenstand von vor seinem Eingriff wieder hergestellt werden kann. Änderungen an Datenständen sind zu versionieren und dokumentieren.

2.6.4 Remote Access

Remote-Access-Anbindungen an das System des Auftraggebers sind untersagt, es sind ausschließlich die vom Auftraggeber bereitgestellten Remote-Access-Anbindungen zu nutzen.

Sind zur Erfüllung des Auftrags Remote-Access Anbindungen notwendig, müssen diese beim Auftraggeber beantragt werden. Die Nutzung genehmigter Remote-Access-Zugänge ist bei Tätigkeiten, die Änderungen in der produktiven Systemlandschaft nach sich ziehen, durch den Dienstleister vorher mit dem WVV-Ansprechpartner abzustimmen.

2.7 Regelungen für Besitzer von Schließberechtigungen

Der Dienstleister hat die Schließberechtigungen beim Auftraggeber zu beantragen. Der Dienstleister muss die Zutrittsmittel sicher verwahren, darf diese nicht an Dritte weitergeben und muss den Verlust unverzüglich gegenüber dem Auftraggeber anzeigen. Nach Abschluss der Dienstleistertätigkeit ist das Zutrittsmittel dem Auftraggeber zurückzugeben.

2.8 Regelungen für den physischen Transport von Informationen

Bei dem physischen Transport von Informationen hat der Dienstleister entsprechende Vorkehrungen nach Stand der Technik einzuhalten, um den Schutz der Informationen zu gewährleisten.