Sicherheitsrichtlinie Informationssicherheit und Datenschutz für IT-Fremddienstleister juwi AG

Richtlinie

Ziel der Richtlinie

Die juwi-Gruppe hat ihre Strategie in Bezug auf den Schutz von Unternehmensinformationen in einer übergeordneten „Leitlinie Informationssicherheit“ festgelegt. Diese soll die Erfüllung der unternehmensinternen Vorgaben an Informationssicherheit und der gesetzlichen Vorschriften sicherstellen.
Aus diesem Grund hat die Informationssicherheitsbeauftragte der juwi AG Anforderungen an und Vorgaben für die Zusammenarbeit mit IT-Dienstleistern (nachfolgend „Auftragnehmern“ genannt) in dieser „Sicherheitsrichtlinie Informationssicherheit und Datenschutz für IT-Fremddienstleister“ beschrieben. Sie gilt für IT-Leistungen aller Art für alle Gesellschaften der juwi-Gruppe (nachfolgend „Auftraggeber“ genannt).

Geltungsbereich

Diese Sicherheitsrichtlinie ist für den Zugang und Zugriff auf IT-Systeme, Dienste, Informationen, Daten und Anwendungen in Netzwerken der juwi-Gruppe (nachfolgend „juwi-Netzwerk“ genannt) verbindlich. Sie gilt auch für den Zutritt zu Gebäuden und Räumen mit IT- bzw. Technikkomponenten.

Im Einzelfall können zusätzliche auftrags- oder systembezogene Sicherheitsrichtlinien ergänzt werden.

Der Auftragnehmer sorgt innerhalb seines Unternehmens und sofern Subunternehmen eingesetzt sind, auch bei diesen für die Einhaltung dieser Sicherheitsrichtlinie.

Verantwortlichkeiten

Für die Herausgabe und Umsetzung sowie das Reporting dieser Richtlinie ist der ISB und der Datenschutz verantwortlich.

1. Begriffe und Abkürzungen

ISB = Informationssicherheitsbeauftragte
juwi-Netzwerk = IT-Systeme, Dienste, Informationen, Daten und Anwendungen in Netzwerken der juwi-Gruppe
Auftragnehmer = IT-Dienstleister selbst, seine Mitarbeiter und seine eingesetzten Subunternehmer und dessen Mitarbeiter

Auftraggeber = eine Gesellschaft der juwi-Gruppe
BSI = Bundesamt für Sicherheit in der Informationstechnik
DSGVO = Datenschutzgrundverordnung
BDSG = Bundesdatenschutzgesetz

2. Allgemeine Bestimmungen

Zutritt zu den Gebäuden und Räumlichkeiten/Büros der juwi-Gruppe sind immer über einen Ansprechpartner der juwi-Gruppe zu beantragen. Im Falle, dass dem Auftragnehmer eine Zutrittskarte ausgehändigt wird, ist dieser verpflichtet, diese immer gut sichtbar bei sich zu führen. Dem Auftragnehmer und/oder Mitarbeiter desselben ist es untersagt, sich unbegleitet in Räumlichkeiten der juwi-Gruppe zu bewegen.

3. Technische Sicherheitsrichtlinien

3.1. Zugangs- und Zugriffsrechte

Zugangs- und Zugriffsrechte für das juwi-Netzwerk werden nach Notwendigkeit gewährt und nach Bedarf eingeschränkt. Die Einrichtung von Zugangs- und Zugriffsrechten für das juwi-Netzwerk erfolgt durch den juwi IT-Support und muss durch den Auftraggeber bei diesem beantragt werden.

Ist für einen Auftragnehmer ein Zugang/Zugriff zum juwi-Netzwerk eingerichtet, sind die nachfolgenden Regelungen zu beachten:

a) Jeder Mitarbeiter des Auftragnehmers muss sich mit der ihm von juwi zugewiesenen Benutzerkennung anmelden. Der Auftraggeber weist den Auftragnehmer darauf hin, dass Zugang und Zugriffe auf das juwi-Netzwerk protokolliert werden. Der Auftragnehmer informiert hierüber seine Mitarbeiter und Subunternehmen. Benutzerkennungen und Kennwörter dürfen nicht weitergegeben werden.
b) Der Auftragnehmer ist verpflichtet, den Auftraggeber umgehend zu informieren, wenn ein Zugang/Zugriff auf das juwi-Netzwerk nicht mehr erforderlich ist (z.B. Auftragsabschluss, Mitarbeiterwechsel, Kündigung oder sonstige Beendigung des Auftrags).

3.2. Administrationsrechte

Werden zur Erfüllung des Auftrags durch den Auftragnehmer Administrationsrechte benötigt, können diese nach Anfrage des Auftragnehmers beim Auftraggeber eingerichtet werden. Sie unterliegen der Arbeitsanweisung „Verwendung von privilegierten Konten“.

Die Einrichtung, Änderung und Löschung von Administrationsrechten für Systeme innerhalb des juwi-Netzwerks erfolgt durch den juwi IT-Support.

Bei juwi beschäftigte System-Administratoren planen, installieren, konfigurieren und pflegen die informationstechnische Infrastruktur. Sie sorgen im Rahmen ihrer Administrationsaufgaben und -rechte für

a) eine sachgerechte Installation,
b) einen störungsfreien Betrieb,
c) eine angemessene Pflege der IT-Systeme und Anwendungen und
d) eine Beachtung der Ziele der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) im Verantwortungsbereich.

Der Auftragnehmer mit Administrationsrechten hat die nachfolgenden Regeln einzuhalten:

a) Die zum Zweck der Erfüllung des Auftrags eingerichteten Administrationsrechte dürfen ausschließlich für den vorgesehenen Zweck verwendet werden. Eine Weitergabe und/oder Übertragung der zur Erfüllung der Aufgaben persönlich zugeordneten Administrationsrechte sowie diesbezüglicher Benutzerkennungen und Passwörter ist untersagt.
b) Werden aus technischen oder organisatorischen Gründen weitergehende Berechtigungen, als für die Erfüllung des Auftrags erforderlich eingerichtet, dürfen dennoch nur die Berechtigungen genutzt werden, die zur Erfüllung des Auftrags zwingend benötigt werden.
c) Der unberechtigte bzw. außerhalb des Auftrags liegende Zugang und Zugriff auf das juwi-Netzwerk des Auftraggebers ist untersagt.
d) Das Überwinden von Schutzmaßnahmen und Verschlüsselungsmechanismen ist untersagt.
e) Bei der Durchführung von Administrationsaufgaben muss auf eine strikte Gewährleistung der Vertraulichkeit, Verfügbarkeit und Integrität des juwi-Netzwerks geachtet werden.
f) Werden aufgrund von personellen, organisatorischen oder technischen Maßnahmen oder Änderungen die Voraussetzungen der Administrationsrechtevergabe in Teilen oder gänzlich nicht mehr erfüllt oder werden Administrationsrechte nicht mehr benötigt, hat dies der Auftragnehmer unverzüglich dem Auftraggeber mitzuteilen.

3.3. Schutz des Informationsverkehrs

Werden zur Erfüllung des Auftrags Informationen auf IT-Systemen des Auftragnehmers – außerhab des juwi-Netzwerks oder in dieses interiert – übertragen und/oder verarbeitet und ggfs. mit dem Auftraggeber und/oder Unternehmen der juwi-Gruppe ausgetauscht, sind zum Schutz der Informationen und des juwi-Netzwerks nachfolgende Schutzmaßnahmen zu beachten:

a) Der Auftragnehmer muss sicherstellen, dass auf der von ihm verwendeten und bereitgestellten Hardware (z.B. PCs, Server, Gateways) die aktuellste Version eines anerkannten sicheren Virenschutzsystems mit einer regelmäßig aktualisierten Virensignatur-Datenbank installiert ist, die Schutz gegen Angriffe duch Schadsoftware (z.B. Viren, Würmer, Trojanische Pferde) insbesondere via E-Mail, Web, mobile Datenträger (z.B. USB-Stick) oder andere Medien bietet, indem sie den Dateizugriff kontrolliert.
b) Werden vertrauliche Informationen zwischen dem juwi-Netzwerk und dem Netzwerk des Auftragnehmers ausgetauscht, sind die Informationen nach dem Stand der Technik zu schützen und/oder muss die Übertragung/Transport über eine sichere Verbindung/Transportweg stattfinden. Für den Austausch streng vertraulicher Informationen ist eine Inhaltsverschlüsselung (Container, Hardwareverschlüsselung) und geschützte Übertragung/Transport Pflicht.
c) Der Auftragnehmer muss über einen definierten Prozess sicherstellen, dass auf der von ihm verwendeten Hardware korrekt lizenzierte Software und regelmäßig aktualisierte Sicherheits-Patsches für die Betriebssystem-Software und Anwendungen installiert sind.

3.4. Verbindung zu IT-Systemen

Erfolgt eine Anbindung von IT-Systemen aus Netzen des Auftragnehmers an das juwi-Netzwerk, sind nachfolgende Regelungen zu beachten:

a) Wenn zum juwi-Netzwerk Verbindungen hergestellt werden, muss der Auftragnehmer sicherstellen, dass sein eigenes Netzwerk keinen unkontrollierten Zugriff durch Dritte auf das juwi-Netzwerk ermöglicht.
b) Der Auftraggeber übernimmt keine Verantwortung für etwaige Schäden an angrenzenden Systemen des Auftragnehmers, die auftreten können während der Auftragnehmer mit dem juwi-Netzwerk verbunden ist.

3.5. Zugang und Zugriff

Zugang und Zugriff sind vom Auftraggeber beim juwi IT-Support zu beantragen.

Vor der Einrichtung von Zugangs- und Zugriffsrechten (siehe 3.2) wurde dem Auftragnehmer der Auftrag erteilt, damit wurde er über diese Sicherheitsrichtlinie informiert. Bei Bedarf informiert der Auftraggeber die Mitarbeiter des Auftragnehmers über diese Sicherheitsrichtlinie sowie über die Verwendung von privilegierten Konten und händigt eine gesonderte „Verpflichtungserklärung auf das Datengeheimnis und die Informationssicherheit“ zur Unterschrift aus. Zugang und Zugriff werden für externe Mitarbeiter auf den Zeitraum der geplanten Dauer des Auftrags, höchstens aber auf zwölf (12) Monate befristet.

Es erfolgt eine Protokollierung und ggfs. Auswertung der Aktivitäten. Der Auftragnehmer informiert hierüber seine Mitarbeiter und Subunternehmen.

3.6. Verwendung von Wireless-Komponenten

Bei Verwendung von Wireless-Komponenten des Auftragnehmers in Räumlichkeiten der juwi-Gruppe dürfen bestehende Betriebseinrichtungen nicht beeinträchtigt werden und keine Verbindungen zum juwi-Netzwerk hergestellt werden.

3.7. Sicherer System- und Anwendungsbetrieb

Werden IT-Systeme, Anwendungen und IT-Infrastrukturen im Auftrag des Auftraggebers durch den Auftragnehmer in Räumlichkeiten der juwi-Gruppe oder des Auftragnehmers betrieben und/oder administriert (Anwendungs-Service-Provider), gelten die nachfolgenden Regelungen:

a) Der Betrieb muss den Anforderungen des Informationsschutzes entsprechen, um als vertrauenswürdig anerkannt zu werden. Hierzu sind insbesondere
   I. die gesetzlichen Anforderungen einzuhalten,
   II. die allgemeingültigen Sicherheitsstandards nach BSI und/oder ISO 27001 zu beachten,
   III. der Stand der Technik zur sicheren Erhebung, Verarbeitung, Speicherung und Aufbewahrung, Weitergabe sowie Löschung/Entsorgung schutzwürdiger Informationen und
   IV. die Anforderungen an Kommunikations- und Eskalationsprozesse bezogen auf informationsschutzrelevante Ereignisse zu beachten.

b) Der Auftragnehmer muss angemessene Vorsichtsmaßnahmen treffen, um die Hardware-Komponenten vor physischen Schäden zu schützen und die Verwendung durch unbefugte Benutzer zu verhindern.

c) Der Auftragnehmer muss die Sicherheit der Betriebsumgebung gewährleisten sowie logische Zugangs- und Zugriffskontrollen implementieren.

d) Beinhaltet der Auftrag die Erhebung, Nutzung oder Verarbeitung personenbezogener Daten im Sinne der Datenschutzgrundverordnung und des Bundesdatenschutzgesetzes, muss der Auftragnehmer alle aufgrund der gesetzlichen Vorgaben erforderlichen Maßnahmen zum Schutz der Daten treffen.

3.8. Softwareentwicklung und -integration

Erbringt der Auftragnehmer Leistungen oder Softwareentwicklung und/oder -integration, sind unter Beachtung dieser Sicherheitsrichtlinie die projektspezifischen Sicherheitsanforderungen umzusetzen, die zwischen Auftraggeber und Auftragnehmer gesondert vereinbart werden.

4. Allgemeine Verpflichtungen

4.1. Nutzung von Informationen des Auftraggebers

Der Auftragnehmer ist verpflichet, die vom Auftraggeber eingeräumten Zutritts-, Zugangs-/Zugriffsrechte auf juwi-Netzwerke ausschließlich im Rahmen seiner vertraglich zu erfüllenden Verpflichtungen zu nutzen.

Sämtliche durch den Auftrag erlangte, nicht öffentlich bekannte Informationen sowie auftragsbedingt erstellte Kopien, Aufzeichnungen und Arbeitsergebnisse sind Eigentum des Auftraggebers und an diesen nach Beendigung des Auftrags heraus- bzw zurückzugeben.

Der Auftragnehmer ist verpflichtet, alle ihm im Zusammenhang mit der Vertragserfüllung zur Kenntnis gelangten Informationen über den Auftraggeber und Unternehmen der juwi-Gruppe, ihre Geschäfts- und Betriebsangelegenheiten und alle Arbeitsergebnisse vertraulich zu behandeln und angemessen gegen eine Kenntnisnahme durch Unberechtigte und nicht vertragsgemäße Nutzung, Vervielfältigung oder Weitergabe zu schützen. Diese Verpflichtungen gelten über die Beendigung des Vertragsverhältnisses hinaus.

Dem Auftragnehmer ist nicht gestattet, sich geschäftliche oder betriebliche, nicht von der juwi-Gruppe öffentlich bekannt gemachte Informationen gleich welcher Art über Auftraggeber und/oder seine Kunden, Lieferanten oder Mitarbeiter anzueignen, für eigene Zwecke zu nutzen oder Kopien oder Aufzeichnungen ingendwelcher Art zu fertigen, soweit dies nicht zur Erfüllung des Auftrags erforderlich ist. Solche Informationen, Kopien, Aufzeichnungen oder Arbeitsergebnisse dürfen auch nicht an Dritte weitergegeben oder Dritten zur Kenntnis gebracht werden.

Vertrauliche Informationen dürfen nur an die Subunternehmen weitergegeben werden, für die der Auftraggeber seine Zustimmung erteilt hat und die auf die Einhaltung der vorliegenden Sicherheitsrichtlinie verpflichtet wurden. Dies ist auf Verlangen des Auftraggebers durch den Auftragnehmer nachzuweisen.

4.2. Datenschutz

Der Auftragnehmer leistet Gewähr, dass er sämtliche geltende Datenschutzgesetze, namentlich die EU-Datenschutzgrundverordnung und das Bundesdatenschutzgesetz 2018 befolgt und dass er alle nach geltendem Recht erforderlichen Genehmigungen im Hinblick auf den Umgang und/oder die Handhabe personenbezogener Daten eingeholt hat. Der Auftragnehmer wird den Auftraggeber von allen Kosten, Ansprüchen, Haftungen und Forderungen freistellen, die dem Auftraggeber im Hinblick auf eine Verletzung dieser Gewährleistung entstehen.

Der Auftragnehmer erklärt hiermit, dass er die **„Hinweise zur Datenverarbeitung für Kunden, Lieferanten und andere Betroffene“** des Auftraggebers erhalten und zur Kenntnis genommen hat. Der Auftragnehmer verpflichtet sich hiermit für den Fall, dass der Betroffene nicht zugleich der Auftragnehmer ist, diese „Hinweise zur Datenverarbeitung für Kunden, Lieferanten und andere Betroffene“ an die Betroffenen weiterzugeben, die im Rahmen dieses Vertragsverhältnisses auf Initiative des Auftragnehmer mit dem Auftraggeber Kontakt haben werden.

Sofern der Auftragnehmer im Rahmen dieses Vertragsverhältnisses als Auftragsverarbeiter im Sinne des Art. 28 DSGVO tätig wird, werden Auftragnehmer und Auftraggeber zuvor eine den gesetzlichen Vorgaben genügende Vereinbarung zur Auftragsverarbeitung abschließen. Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftragnehmer und Auftraggeber als

Gesamtschuldner. Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenen Umstandes ist, soweit die relevanten Daten unter dieser Vereinbarung erarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftragnehmer den Auftraggeber auf erste Anforderung von sämtlichen Ansprüchen, Forderungen, Haftungen Dritter bzw. gegenüber Dritten sowie Kosten frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber erhoben werden. Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer schuldhaft verursacht. Der Punkt 4.2 Datenschutz gilt nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Leistungen oder einer vom Auftraggeber erteilten Weisung entstanden ist.

Der Auftragnehmer verpflichtet sich, nur Mitarbeiter einzusetzen, die auf das Datengeheimnis gemäß § 5 BDSG (alt) oder zur Wahrung der Vertraulichkeit im Sinne der DSGVO verpflichtet wurden und diese Verpflichtung auch für die Zeit nach ihrem Ausscheiden aus dem Arbeitsverhältnis mit dem Auftragnehmer gilt.

Eine Weitergabe personenbezogener Daten des Auftraggebers durch den Auftragnehmer an Dritte bedarf, ungeachtet der gesetzlichen Voraussetzungen, in jedem Fall der vorherigen schriftlichen Zustimmung des Auftraggebers. Der Auftragnehmer verpflichtet sich, Subunternehmer nur dann mit der Verarbeitung von personenbezogenen Daten des Auftraggebers zu betrauen, wenn diese sich zuvor schriftlich in gleicher Weise wie der Auftragnehmer zur Einhaltung der Verpflichtungen nach diesem Punkt 4.2 Datenschutz verpflichtet haben.

4.3. Persönliche Eignung und fachliche Qualifikation der Mitarbeiter

Der Auftragnehmer ist verpflichtet, ausschließlich Mitarbeiter beim Auftraggeber einzusetzen, die persönlich geeignet und fachlich qualifiziert sind. Die Beurteilung der Mitarbeiter ist vor Beginn des Auftragsverhältnisses durch den Auftragnehmer sicherzustellen.

Es ist durch den Auftragnehmer sicherzustellen, dass Mitarbeiter, deren persönliche und/oder fachliche Eignung als nicht ausreichend bewertet werden können, weder Zutritt auf das Gelände oder in die Gebäude, noch Zugang zum juwi-Netzwerk des Auftraggebers erhalten.

Auf Anfrage des Auftraggebers legt der Auftragnehmer dem Auftraggeber geeignete Unterlagen zur Überprüfung der persönlichen und fachlichen Eignung vor.

Der Punkt 4.3 gilt entsprechend für Mitarbeiter von Subunternehmen.

5. Kontrolle der Einhaltung der Sicherheitsrichtlinien, Meldepflicht und Zugangs- und Zugriffssperrung

Der Auftraggeber hat das Recht, die Einhaltung dieser Sicherheitsrichtlinie auch am Standort des Auftragnehmers zu kontrollieren. Der Auftragnehmer hat dem Auftraggeber ferner die Kontrolle an den Standorten seiner Subunternehmer zu ermöglichen.

Der Auftragnehmer ermöglicht dem Auftraggeber insbesondere nach vorheriger Benachrichtigung und innerhalb der normalen Geschäftszeiten Zutritt zu allen relevanten Betriebsstandorten und unterstützt ihn bei allen erforderlichen Aktivitäten und Tests. Er gewährt darüber hinaus Einsicht in, für das juwi-Netzwerk betriebsrelevante Dokumentationen.

Des Weiteren behält sich der Auftraggeber das Recht vor, die Art des Zugangs/Zutritts des Auftragnehmers auf das juwi-Netzwerk zu modifizieren, um die Sicherheit des juwi-Netzwerks zu gewährleisten.

Der Auftragnehmer ist verpflichtet, die für ihn einschlägigen Sicherheitsregelungen und Gesetze einzuhalten, sämtliche relevanten Fehler, Unregelmäßigkeiten oder Sicherheitsvorfälle sowie eingeleitete Maßnahmen zu deren Behebung im Zusammenhang mit dem juwi-Netzwerk revisionssicher zu dokumentieren und dem Auftraggeber unverzüglich zu melden.