Informationssicherheitsanforderungen an Auftragnehmer

Version: 02.09.2024

Begriff [Abkürzung]	Definition
AN	Auftragnehmer
Informationsverarbeitende Einrichtung	Sämtliche Netz- und Informationssysteme aus dem Bereich IT und OT
ISMS	Informationssicherheitsmanagementsystem
IT	Information Technology
NISG	Netz- und Informationssystemsicherheitsgesetz, BGBl. I Nr. 111/2018
NISV	Netz- und Informationssystemsicherheitsverordnung, BGBl. II Nr. 215/2019
OT	Operational Technology
TAG GmbH	TAG GmbH, eingetragen im Firmenbuch des Handelsgerichts Wien unter FN 122567x, mit Sitz in Wien und Geschäftsanschrift in der Wiedner Hauptstraße 120, 1050 Wien.

Lieferanten und Kontraktoren (allgemein Auftragnehmer, nachfolgend als "AN" bezeichnet) haben im Rahmen der Leistungserbringung für die TAG GmbH nachfolgende Informationssicherheits-anforderungen einzuhalten. Insbesondere betreffen die Anforderungen jene AN, an die der Betrieb von informationsverarbeitenden Einrichtungen im Zusammenhang mit dem wesentlichen Dienst der TAG GmbH gemäß NISG ausgelagert ist bzw. AN mit (administrativem) Zugriff auf informationsverarbeitende Einrichtungen der TAG GmbH.

Anforderung	Regelung
Allgemein	**Der AN verpflichtet sich in Bezug auf die Leistungserbringung für die TAG GmbH folgende Regelungen einzuhalten, und Maßnahmen bzw. technische Standards umzusetzen. Weiters akzeptiert und anerkennt der AN rechtsgültig in Bezug auf die Leistungserbringung für die TAG GmbH die hierin festgeschriebenen Rechte der TAG GmbH.**

Informationssicherheitsmaßnahmen und Informationssicherheitsmanagement	Einhaltung der Sicherheitsmaßnahmen gemäß Netz- und Informationssystemsicherheitsverordnung – "NISV" in Bezug auf die Leistungserbringung für die TAG GmbH. Abgestimmte Umsetzung der Informationssicherheitsanforderungen und technischen Standards (in Bezug auf Informationssicherheit) der TAG GmbH. Betrieb eines zertifizierten Informationssicherheitsmanagementsystems (ISMS) gemäß anerkannter Standards (z.B. ISO/IEC 27001) und Umsetzung von Informationssicherheitsmaßnahmen nach dem Stand der Technik.
Subauftragnehmer	Verbindliche Weitergabe und Überbindung der Informationssicherheitsanforderungen der TAG GmbH an Subauftragnehmer. Auf Verlangen der TAG GmbH ist vom AN ein entsprechender Nachweis zu erbringen.
Zugriff auf Informationen und informationsverarbeitende Einrichtungen der TAG GmbH	Zugriff (des eingesetzten Personals) ausschließlich nach dem Need-to-know-Prinzip (Beschäftigte des AN erhalten Zugang zu den Informationen und Anlagen der TAG GmbH in dem Umfang, der für die Leistungserbringung benötigt wird) und Least-Privilege-Prinzip (kein Zugang zu Informationen und Anlagen der TAG GmbH über den vorgenannten Bedarf und dem damit verbundenen Zeitraum hinaus). Pflicht zur unverzüglichen Mitteilung, wenn Beschäftigte des AN, die Zugriff auf informationsverarbeitende Einrichtungen der TAG GmbH haben, das Unternehmen des AN verlassen oder innerhalb des Unternehmens des AN die Position wechseln und sich daraus Änderungen im Zusammenhang mit der Leistungserbringung für die TAG GmbH ergeben.
Gebrauch geheimer Authentisierungsinformationen	Zugriff auf informationsverarbeitende Einrichtungen der TAG GmbH nur mittels je Benutzer und Anwendung individuell vergebener Authentisierungsinformationen (insbesondere Passwörter); die Mehrfachverwendung derselben Authentisierungsinformationen für andere Zwecke (u.a. für andere Benutzer, Anwendungen oder bei anderen Kunden des AN) ist untersagt. Pflicht zur Änderung vergebener Initialpasswörter bei der ersten Verwendung.
Sicherheitsüberprüfung des eingesetzten Personals	Durchführung und Nachweis von Sicherheitsüberprüfungen von Schlüsselpersonal im Zusammenhang mit der Leistungserbringung für die TAG GmbH.
Physischer Zutritt bei Leistungserbringung an einem Standort der TAG GmbH	(Erstmaliger) Zutritt erst nach nachweislich erfolgter Unterweisung betreffend die Informationssicherheitsregeln der TAG GmbH.

Einbringung externer Hardware	Externe Hardware des AN (z.B. Wartungs-Laptop) darf nur bei betrieblicher Notwendigkeit und nach erfolgter Freigabe der TAG GmbH mit den informationsverarbeitenden Einrichtungen der TAG GmbH verbunden werden. Der AN hat unaufgefordert nachzuweisen, dass die betroffene Hardware über dem Stand der Technik entsprechende Sicherheitsmaßnahmen verfügt.
Handhabung und Übertragung von Informationen	Anwendung der Regelungen der TAG GmbH zur Klassifizierung von Informationen. Pflicht zur Rückgabe überlassener Informationen der TAG GmbH (inkl. jegliche zur Nutzung überlassene Hardware und Software) sowie von Einrichtungen der TAG GmbH, die einen Zugriff auf bzw. einen Zugang zu Informationen und Anlagen der TAG GmbH ermöglichen (z.B. Schlüssel, Zutrittskarten, Security-Token).
Fernzugriff/Fernwartungstätigkeiten betreffend informationsverarbeitende Einrichtungen der TAG GmbH	Zulässige Methoden für den Fernzugriff auf informationsverarbeitende Einrichtungen sind gemeinsam mit TAG GmbH zu definieren. Administrative Fernwartungstätigkeiten, soweit möglich, nur nach vorher erfolgter Genehmigung und/oder Freischaltung durch TAG GmbH (sowie Deaktivierung nach Abschluss der Fernwartungstätigkeiten). Zeitlich begrenztes Recht auf Fernzugriffe (z.B. 1 Jahr); wiederkehrende Verlängerung durch TAG GmbH nach Evaluierung (Erforderlichkeit, Rechteumfang etc.). Recht auf Protokollierung der Fernzugriffe und Auswertung der Protokolle durch die TAG GmbH.
Lieferantenaudits	Recht der TAG GmbH auf die regelmäßige Durchführung von Informationssicherheitsaudits und Inspektionen durch die TAG GmbH bzw. von der TAG GmbH beauftragte Dritte.
Laufende Überwachung der Tätigkeiten im Rahmen der Lieferantenvereinbarung	Rechte der TAG GmbH zur Überprüfung und Überwachung von Aktivitäten, die vertrauliche Informationen sowie die informationsverarbeitenden Einrichtungen der TAG GmbH berühren (z.B. Logging und Log-Auswertung).
Sicherheitsvorfälle	Pflicht zur unverzüglichen Meldung von Sicherheitsvorfällen sowie von Vorfällen, die den wesentlichen Dienst der TAG GmbH betreffen, an security@taggmbh.at sowie, sofern vereinbart, weitere definierte Kontakte gemäß den Rahmenbedingungen aus NISG und NISV, insbesondere unter Nennung eines Ansprechpartners beim AN inkl. Kontaktinformationen. Vereinbarung gemeinsam mit TAG GmbH von Reaktions- und Wiederherstellungsprozessen nach Sicherheitsvorfällen und regelmäßiger Überprüfung derselben. Pflicht zur laufenden und abschließenden Berichterstattung an die TAG GmbH über die Bewältigung von Sicherheitsvorfällen.

Berichtspflichten	Regelmäßige (zumindest jährliche) Berichterstattung zum Status der Informationssicherheit im Zusammenhang mit der Leistungserbringung für die TAG GmbH an security@taggmbh.at sowie, sofern vereinbart, weitere definierte Kontakte. Sofern anwendbar: Berichterstattung über Ergebnisse, • die die Leistungserbringung für die TAG GmbH betreffen, • der Überprüfungen durch qualifizierte Stellen gemäß NISG.
Geheimhaltungsvereinbarungen	Eine Geheimhaltungsvereinbarung mit TAG GmbH entsprechend dem TAG GmbH Standard ist verpflichtend abzuschließen.
Änderung der Lieferantenvereinbarung	Diese Mindestsicherheitsanforderungen sind auf Grund veränderter gesetzlicher Rahmenbedingungen (v.a. Änderung NISG, NISV) von Zeit zu Zeit in beidseitigem Einvernehmen anzupassen.