Richtlinie

Informationssicherheit für externe Parteien

Inhalt

1. Zweck

Diese Richtlinie definiert Informationssicherheitsanforderungen an externe Parteien (Lieferanten und andere Geschäftspartner), um die Sicherheit von DRÄXLMAIER-Informationen im Rahmen der Zusammenarbeit zu gewährleisten. Sie richtet sich an Dritte, denen Zugang zu informationstechnischen (IT)-Services von DRÄXLMAIER gewährt wird.

Die externe Partei hat dafür Sorge zu tragen, dass alle in dieser Richtlinie definierten technischen und organisatorischen Maßnahmen umgesetzt sind und das Personal vor dem Zugriff auf DRÄXLMAIER IT-Services ordnungsgemäß eingewiesen wird.

2. Geltungsbereich

Diese Richtlinie gilt für alle externen Parteien, denen Zugang zu DRÄXLMAIER IT-Dienstleistungen gewährt wird. Die externe Partei bestätigt die Einhaltung der Vorgaben als Teil der vertraglichen Vereinbarung.

3. Begriffe, Abkürzungen & Rollen

Begriff	Erklärung
DRÄXLMAIER	Die DRÄXLMAIER Gruppe (https://www.draexlmaier.com) inkl. aller Tochtergesellschaften und insbesondere die DRÄXLMAIER Gesellschaft, die Vertragspartner in der Geschäftsbeziehung mit der externen Partei ist.
DRÄXLMAIER Information	Nicht-öffentliche Informationen (digital, verbal, physisch), die durch DRÄLXMAIER mit der externen Partei im Rahmen der Geschäftspartnerschaft geteilt werden. Informationen, die öffentlich zugänglich sind, fallen nicht unter diesen Begriff.
DRÄXLMAIER IT-Services	Umfasst digitale Dienste und Portale, die von oder im Auftrag von DRÄXLMAIER erbracht werden und bei denen die externe Partei bzw. deren Mitarbeiter Zugangsdaten erhalten hat bzw. haben. Dazu gehören unter anderem das Lieferantenportal der DRÄXLMAIER Group, der Zugang zum DRÄXLMAIER Netzwerk und der Zugang zu DRÄXLMAIER Collaboration Services.
DRÄXLMAIER Netzwerk	Abgegrenztes IT-Netzwerk, das alle DRÄXLMAIER-Standorte und IT-Geräte für eine sichere Datenkommunikation verbindet.
Abkürzungen	Alle relevanten Abkürzungen finden Sie zentral im D-World Abkürzungsverzeichnis. D-World -> Worldwide -> Service -> Abkürzungsverzeichnis

Rolle	Erklärung
Externe Partei	Jedes Unternehmen bzw. jede Person, das bzw. die in Geschäftsbeziehung zu einer Tochtergesellschaft der DRÄXLMAIER Gruppe oder einem ihrer verbundenen Unternehmen steht (siehe http://www.draexlmaier.com für Details). Dazu gehören unter anderem Lieferanten, Kunden, Forschungseinrichtungen, Behörden.
DRÄXLMAIER Kontakt	Auftraggeber und/oder Einkäufer bei DRÄXLMAIER.

4. Inhalte der Richtlinie

4.1 Information Security Management System (ISMS)

Die externe Partei muss interne Richtlinien, Verfahren und organisatorische Verantwortlichkeit implementieren, um die Sicherheit von bereitgestellten DRÄXLMAIER-Informationen zu gewährleisten. Der Aufbau der Organisation, der Richtlinien und Verfahren soll sich an etablierten Sicherheitsstandards orientieren, z.B. ISO 27001 oder NIST Cybersecurity Framework und so den Schutz von DRÄXLMAIER Informationen im Rahmen der Geschäftspartnerschaft wirksam unterstützen.

4.2 Unterweisung

Alle Mitarbeiter der externen Partei mit Zugang zu DRÄXLMAIER IT-Services sind gemäß Anhang A "Informationssicherheitsanweisungen für Externe" und den Regelungen dieser Vereinbarung zu unterweisen. Die externe Partei ist dafür verantwortlich, die erfolgreiche Unterweisung und Schulung ihrer Mitarbeiter sicherzustellen. Die Unterweisung muss schriftlich dokumentiert und mindestens jährlich erneuert werden. Die externe Partei verpflichtet sich im Namen ihres Personals, dass die Anweisungen befolgt werden.

4.3 Umgang mit DRÄXLMAIER Informationen

DRÄXLMAIER praktiziert die Informationsklassifikation nach der Empfehlung des VDA "Harmonisierung der Klassifizierungsstufen". Sofern nicht anders angegeben, ist die Standardeinstufung von DRÄXLMAIER-Informationen "vertraulich".

4.4 Umgang mit DRÄXLMAIER IT-Services

Information, die im Rahmen des Zugriffs auf DRÄXLMAIER IT-Services zur Verfügung gestellt wird, ist durch eine Geheimhaltungsvereinbarung geschützt und soll nur mit gesicherten DRÄXLMAIER IT-Diensten verarbeitet werden. Dabei ist Folgendes einzuhalten:

4.4.1 Zugriffsberechtigung

Für den Zugriff auf DRÄXLMAIER IT-Services wurden Zugangsdaten (z.B. Benutzername und Passwort, Sicherheitstoken) an Mitarbeiter der externen Partei vergeben. Änderungen der Verantwortlichkeiten oder des Personals auf Seiten der externen Partei sind dem Ansprechpartner bei DRÄXLMAIER zur Anpassung der Zugriffsberechtigungen und zur Sicherstellung des Need-to-know-Prinzips unverzüglich schriftlich mitzuteilen.

4.4.2 Zugangsdaten

Die Weitergabe individuell zugewiesener Benutzerdaten und weiterer Sicherheitsfaktoren (Passwort, Sicherheitstoken bzw. Ausweis) ist nicht zulässig. Die externe Partei muss den sicheren Umgang mit Zugangsdaten unterstützen, indem sie ihren Mitarbeitern Prozesse und Tools zur Verfügung stellt, um eine korrekte Handhabung von Passwörtern und anderen Sicherheitsfaktoren zu ermöglichen.

4.4.3 Extrahieren von Informationen

Es ist untersagt, Informationen aus DRÄXLMAIER IT-Services zu extrahieren (z.B. durch Screenshots, Fotografien, Videoaufzeichnungen, Downloads, manuelle oder automatisierte E-Mail-Weiterleitung etc.), es sei denn, die externe Partei wird dazu ausdrücklich schriftlich aufgefordert.

4.4.5 Bestimmungsgemäße Nutzung

Alle IT-Services werden ausschließlich zum Zwecke der Erfüllung vertraglicher Verpflichtungen gegenüber DRÄXLMAIER bereitgestellt. Eine Verwendung für andere Zwecke ist nicht gestattet.

4.5 Absicherung von Endgeräten

Alle Geräte, die für den Zugriff auf DRÄXLMAIER IT-Services verwendet werden, einschließlich derjenigen, die sich im Besitz der externen Partei befinden, müssen sorgfältig gewartet werden, um sicherzustellen, dass sie kein Sicherheitsrisiko darstellen. Dazu gehört mindestens, dass die Geräte über einen effektiven Schutz gegen Schadsoftware verfügen, eine definierte Sicherheitskonfiguration aufweisen, dass Sicherheitsupdates zeitnah installiert werden und dass die Geräteintegrität (Sollzustand) überwacht wird.

4.6 Einbindung von Fremdgeräten

Die Integration von IT-Geräten, welche nicht unter der vollständigen Verwaltung von DRÄXLMAIER stehen (Fremdgeräte), in das DRÄXLMAIER-Netzwerk ist nicht gestattet. Beinhaltet die Geschäftsbeziehung die Lieferung/Installation solcher Geräte, so unterliegt deren Integration und Nutzung den "Allgemeinen Technischen Liefervorschriften (ATLV) DRÄXLMAIER Group".

4.7 Abgesicherter Datenaustausch

Eine Übertragung von Daten an oder von DRÄXLMAIER IT-Services ist zu unterlassen, es sei denn, dies wurde ausdrücklich angewiesen. Für die allgemeine E-Mail-Kommunikation wird empfohlen, eine gesicherte Verbindung zwischen E-Mail-Servern zu aktivieren, indem die Transportverschlüsselung als obligatorisch aktiviert wird. Einzelheiten hierzu können über den bekannten DRÄXLMAIER Kontakt erfragt werden.

4.8 Standortbesuche

Das Personal der externen Partei welches einen DRÄXLMAIER-Standort besucht, muss die Anweisungen, für Besucher, die bei der Erstregistrierung zur Verfügung gestellt werden, vollständig befolgen. Es ist nicht gestattet, zusätzliches Personal ohne ordnungsgemäße Registrierung auf das Firmengelände mitzunehmen oder Fotos, Video- oder Audioaufnahmen zu anzufertigen.

4.9 Meldung von Sicherheitsvorfällen

Ein Sicherheitsvorfall ist jedes Ereignis, das die Vertraulichkeit, Integrität oder Verfügbarkeit von DRÄXLMAIER-Informationen einschließlich der bereitgestellten Zugangsdaten gefährden könnte. Hat die externe Partei Grund zu der Annahme, dass auf ihrer Seite ein Sicherheitsvorfall aufgetreten ist, bei dem nicht ausgeschlossen werden kann, dass DRÄXLMAIER betroffen ist, sind der DRÄXLMAIER Kontakt und die DRÄXLMAIER IT unter itcc@draexlmaier.com unverzüglich zu benachrichtigen.

4.10 Überprüfung der Einhaltung

DRÄXLMAIER behält sich das Recht vor, die Einhaltung der in dieser Richtlinie und den mitgeltenden Dokumenten festgelegten Vorschriften zu überprüfen. Hierfür kann eine Prüfung am Standort des Fremdunternehmens, an DRÄXLMAIER Standorten oder telefonbasiert erfolgen. Die Prüfung kann von einem autorisierten Dritten im Auftrag von DRÄXLMAIER durchgeführt werden. Die externe Partei hat alle Prüfungstätigkeiten entsprechend zu unterstützen. Gegebenenfalls akzeptiert DRÄXLMAIER auch gültige Sicherheitszertifikate als Nachweis.

4.11 Einbindung von Unterauftragnehmern

Die Einbindung von Unterauftragnehmern richtet sich nach den Vertragsbedingungen, die im Rahmen der Geschäftspartnerschaft festgelegt sind. Wird Dritten über die externe Partei Zugang zu DRÄXLMAIER IT-Services gewährt, so hat die externe Partei eine vollumfängliche vertragliche Verpflichtung aller Unterauftragnehmer auf die in dieser Richtlinie festgelegten Regelungen sicherzustellen. Eine Weitergabe von DRÄXLMAIER Informationen als Agent (Extrahieren von Daten und Weiterleiten an den Unterauftragnehmer) ist nicht gestattet (siehe Ziffer 4.4.3).

4.12 Ende der Geschäftsbeziehung

Bei Beendigung der Geschäftsbeziehung (z.B. alle Leistungen/Waren geliefert) endet die Berechtigung zum Zugang zu den IT-Services von DRÄXLMAIER. DRÄXLMAIER wird die Deaktivierung relevanter Konten einleiten. Die externe Partei stimmt zu, den Zugang nicht mehr zu nutzen und alle zur Verfügung gestellten Arbeitsmaterialien (z.B. IT-Geräte, Zugangskarten etc.) unverzüglich an DRÄXLMAIER zurückzugeben.

4.13 Haftung

Für den Fall, dass der Auftragnehmer die Pflichten aus dieser Richtlinie verletzt, hat er der DRÄXLMAIER Group die dadurch entstehenden Schäden, Kosten und/ oder Aufwendungen zu ersetzen.

5. Mitgeltende Dokumente

Name	Beschreibung
LIEP	Leitfaden Informationssicherheit für externe Parteien

6. Änderungshistorie

Letzte Änderung:

Die vorige Richtlinie „Information Security Directive for External Companies and Partners" wurde durch das vorliegende Dokument ersetzt und der Geltungsbereich auf Externe mit IT-Zugang angepasst.

Version	Beschreibung der Änderung	Bearbeiter	Änderungsdatum
1	Neuerstellung	R. Pöhlmann	01.12.2021