

# Informationssicherheitsrichtlinie für IT-Auftragnehmer (Extern)

Diese Richtlinie gilt für alle externen Auftragnehmer, Lieferanten und Dienstleister sowie deren Mitarbeiter, die Zugriff auf Informationen, Daten oder IT-Systeme der Scheuch-Gruppe erhalten.

Sie ergänzt die jeweils gültigen Allgemeinen Einkaufsbedingungen sowie sonstige vertragliche Vereinbarungen und regelt ausschließlich besondere Anforderungen der Informations- und IT-Sicherheit in einem eigenständigen Dokument.

## Zweck und Zielsetzung

Zweck dieser Richtlinie ist die Sicherstellung eines einheitlichen Sicherheitsniveaus beim Umgang externer Dritter mit Informationen, Daten und IT-Systemen der Scheuch-Gruppe. Sie dient dem Schutz der Vertraulichkeit, Integrität und Verfügbarkeit aller informationsverarbeitenden Werte vor unbefugtem Zugriff, Verlust oder Missbrauch.

### 1. Zugriffskontrolle und Identitätsmanagement

- a) Least Privilege Prinzip: Der Zugriff wird nur auf die Daten und Systeme beschränkt, die für die Erfüllung der vertraglichen Aufgabe zwingend notwendig sind.
- b) Persönliche Accounts: Zugangsdaten (User-IDs) sind personengebunden und dürfen nicht geteilt werden.
- c) Zwei-Faktor-Authentifizierung (2FA): Bei Fernzugriffen (VPN) ist eine 2FA zwingend erforderlich.
- d) Beendigung: Bei Beendigung des Auftragsverhältnisses ist der Zugriff unverzüglich zu entziehen.

### 2. Sicherheitsanforderungen an IT-Assets

- a) Unternehmenseigene Geräte: Werden Geräte von der Scheuch Gruppe genutzt, dürfen keine privaten Anwendungen installiert oder Einstellungen verändert werden.
- b) Bring Your Own Device (BYOD): Werden eigene Geräte genutzt, müssen diese den Sicherheitsstandards entsprechen (Verschlüsselung, aktueller Virenschutz, Firewall, zeitnahe Patch-Installation).
- c) Wechselmedien: Die Nutzung von USB-Sticks oder externen Festplatten ist grundsätzlich untersagt, sofern nicht explizit genehmigt.

### 3. Sichere Arbeitsweise

- a) Sperrung: Arbeitsplätze müssen bei Verlassen sofort gesperrt werden (Windows + L).
- b) Entsorgung: Physische Dokumente sind datenschutzkonform (Schredder) zu vernichten.
- c) Passwörter: Es sind starke, eindeutige Passwörter zu verwenden.

### 4. Incident Management (Sicherheitsvorfälle)

- a) Meldepflicht: Sicherheitsvorfälle (z.B. Phishing, Datenverlust, kompromittierte Geräte, unbefugter Zugriff) müssen unverzüglich (innerhalb von 1 Stunde) an Michael Stelzer/IT-Security-Team gemeldet werden.
- b) Zusammenarbeit: Im Falle eines Vorfalls ist der Auftragnehmer verpflichtet, bei der Aufklärung vollumfänglich zu kooperieren.

### 5. Abnahme und Einverständnis

Der Auftragnehmer bestätigt durch seine Unterschrift, diese Richtlinie gelesen und verstanden zu haben und verpflichtet sich, die Sicherheitsmaßnahmen strikt einzuhalten.

Ort, Datum: \_\_\_\_\_

Name & Unterschrift Auftragnehmer: \_\_\_\_\_