

# Information Security Policy for IT Contractors (External)

This policy applies to all external contractors, suppliers, and service providers, as well as their employees, who are granted access to information, data, or IT systems of the Scheuch Group.

It supplements the currently valid General Terms and Conditions of Purchase as well as other contractual agreements and exclusively governs specific information and IT security requirements in a separate document.

## Purpose and Objectives

The purpose of this policy is to ensure a uniform level of security when external third parties handle information, data, and IT systems of the Scheuch Group.

It serves to protect the confidentiality, integrity, and availability of all information-processing assets against unauthorized access, loss, or misuse.

## 1. Access Control and Identity Management

**a) Principle of Least Privilege:** Access is restricted exclusively to the data and systems that are strictly necessary for fulfilling the contractual task.

**b) Personal Accounts:** Access credentials (user IDs) are assigned to individuals and must not be shared.

**c) Two-Factor Authentication (2FA):** 2FA is mandatory for remote access (VPN).

**d) Termination:** Upon termination of the contractual relationship, access must be revoked immediately.

## 2. Security Requirements for IT Assets

**a) Company-Owned Devices:** If devices provided by the Scheuch Group are used, no private applications may be installed and no system settings may be modified.

**b) Bring Your Own Device (BYOD):** If personal devices are used, they must comply with security standards (encryption, up-to-date antivirus protection, firewall, timely installation of patches).

**c) Removable Media:** The use of USB flash drives or external hard drives is generally prohibited unless explicitly approved.

## 3. Secure Working Practices

**a) Locking:** Workstations must be locked immediately when left unattended (Windows + L).

**b) Disposal:** Physical documents must be destroyed in compliance with data protection requirements (shredding).

**c) Passwords:** Strong, unique passwords must be used.

## 4. Incident Management (Security Incidents)

**a) Reporting Obligation:** Security incidents (e.g., phishing, data loss, compromised devices, unauthorized access) must be reported immediately (within 1 hour) to Michael Stelzer / the IT Security Team.

**b) Cooperation:** In the event of an incident, the contractor is obligated to fully cooperate in the investigation.

## 5. Acceptance and Consent

By signing, the contractor confirms that they have read and understood this policy and agrees to strictly comply with the security measures.

**Location, Date:** \_\_\_\_\_

**Name & Signature of Contractor:** \_\_\_\_\_