Verhaltensvorschriften für Externe

1. Grundsätzliches

Die nachfolgenden Bestimmungen enthalten Verhaltensvorschriften (Aufgaben und Verantwortlichkeiten) für Personen, die in keinem Arbeitsverhältnis zu SIX stehen, sich jedoch im Rahmen ihres Auftrages in den Räumlichkeiten von SIX aufhalten und insbesondere mit geschäftlichen Informationen und Daten sowie Computer-Einrichtungen und Unterlagen zu tun haben (nachfolgend „Externe“ genannt).

2. Verhaltensvorschriften

Externe sind verpflichtet, die zur Kenntnis gebrachten Weisungen und Merkblätter von SIX sowie allfällige Vorgaben von einzelnen Geschäftseinheiten zu befolgen. Die folgenden Regeln sind unbedingt einzuhalten:

- Das Anschliessen von Arbeitsstationen, Notebooks oder anderen technischen Geräten von Dritten (Kunden, Partner, Lieferanten usw.) an das Netz von SIX ist verboten. Ausnahmebewilligungen sind vorab durch Corporate Security zu genehmigen.
- Die für den Zugriff auf Systeme und Daten von SIX vorgesehenen Identifikations-, Authentisierungs- und Arbeitsmittel wie UserID, Passwort, Token, Notebook usw. sind persönlich und dürfen nicht an Dritte weitergegeben, ihnen anderweitig zugänglich gemacht oder privat verwendet werden.
- Jeder Externe ist verantwortlich für die mit seinem Account ausgeführten Tätigkeiten.
- Alle Informationen und Daten sind zu klassifizieren.
- Passwörter (Chiffrierschlüssel) sind getrennt von den chiffrierten Daten aufzubewahren und zu versenden.
- Die lokal auf den Computer-Einrichtungen oder mobilen Datenträgern abgelegten oder transferierten geschäftlichen Daten müssen (mit Ausnahme von intern und öffentlich klassifizierten Daten) chiffriert sein.
- Alle im Rahmen des Auftrags erhaltenen und erzeugten Informationen und Daten sind regelmässig auf Systemen der SIX zu sichern (Backup).
- Datenträger und von SIX Group-fremden Quellen importierte Daten und Programme müssen vor Gebrauch sowie vor Abgabe oder Übermittlung an Dritte mit einem aktuellen Virenscanner auf Viren und Trojaner geprüft werden.
- Die Informationen und Informationsträger bzw. Daten und Datenträger für Ton, Schrift und Bild (z. B. Papiernotizen, Sprachaufzeichnungen, Film- oder Druck-Output) sind nach Beendigung des Gebrauchs oder spätestens mit Ende des Mandats zurückzugeben oder sicher zu vernichten resp. zu entsorgen.
- Die Nachvollziehbarkeit aller Aktivitäten (wie Bearbeitungen von Daten und Programmen oder Veränderung von Konfigurationen) muss jederzeit gewährleistet sein.
- Bei allfälligem Missbrauch, Verlust oder Diebstahl von Systemen, Komponenten oder Daten von SIX ist die zugewiesene SIX Kontaktperson unverzüglich zu informieren.
- Zusätzliche Details zu betrieblichen Richtlinien können folgenden Dokumente des internen Rechts entnommen werden::
    - Compliance Weisung 5: Geheimhaltung im Konzern
    - CRO Reglement C4: Handhabung und Schutz von Informationen
    - Compliance Weisung 1: Datenschutz
    - CRO Reglement S2: Informationssicherheit
    - CRO Reglement S2 Anhang 4: Informationsmanagement
    - CFO Reglement 13: Identity and Access Management
    - IT Standard: Password-Based Authentication

3. Bestätigung durch die Externe Person

Der/die Externe bestätigt durch seine/ihre Unterschrift, dass er/sie diese Verhaltensvorschriften zur Kenntnis genommen und akzeptiert hat.

Ort / Datum: _____

Firma: _____

Unterschrift: _____

Name in Druckbuchstaben: _____

Kontaktadresse für inhaltliche Fragen: corporate-security@six-group.com