



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 Divisionen 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. Ausnahmegenehmigungen 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 Virenschanner 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 Weisungen entnommen werden:
 - Group-Weisungen 1.5 (Geheimhaltung im Konzern), 1.9 (Grundlagen der Behandlung und des Schutzes von Informationen und Geschäftsunterlagen), 1.10 (Behandlung und Schutz von Personendaten), 1.13 (Klassifizierung und Handhabung von Informationen bezüglich Vertraulichkeit) inkl. Anhang 1.
 - Group Weisung 5.2 (Integrale Sicherheit in der SIX Group, insb. Anhang 5a Authentisierung und Autorisierung sowie Anhang 7 Klassifizierung von Informationen bezüglich Integrität, Verfügbarkeit und Verbindlichkeit).

3. BESTÄTIGUNG DURCH DEN EXTERNEN

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

Ort/Datum: _____

Firma: _____

Unterschrift: _____

Name in Druckbuchstaben: _____

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