Sicherheitshinweise für mobile Geräte

Bitte beachten Sie auf jeden Fall diese Sicherheitshinweise, wenn Sie mobile Geräte dienstlich verwenden.

Unabhängig davon, ob Sie es sich um eigene oder Geräte der Firma handelt.

Bewahren Sie Ihre Geräte physisch sicher auf!

01 **Lassen Sie Ihr Notebook oder Smartphone an öffentlichen Orten niemals unbeaufsichtigt!**

02 Verwenden Sie ein starkes und eindeutige Passwörter, die biometrische Authentifizierung, um Ihr Gerät zu sperren oder zu entsperren.

03 Wenn möglich, verwenden Sie ein Kabelschloss, um Ihr Notebook an einem Schreibtisch oder anderen festen Gegenständen zu befestigen.

04 Speichern Sie sensible Daten nicht auf externen Laufwerken oder USB-Sticks, die leicht verlegt oder gestohlen werden können.

05 Bei Verlust eines Gerätes sind die IT-Abteilung unseres Unternehmens oder Ihr Vorgesetzter SOFORT zu verständigen.

Achten Sie auf Datensicherheit!

01 **Erstellen Sie regelmäßig Backups.**

02 Alle Speichermedien, sowohl die internen als auch externe USB-Speicher **MÜSSEN** verschlüsselt werden.

03 Alle Daten sind **ausschließlich** auf den Servern unseres Unternehmens oder in der dafür vorgesehenen Firmen-Cloud zu speichern.

Achten Sie auf eine gute Passwort-Hygiene!

01 **Erstellen Sie sichere, eindeutige Passwörter für alle Konten und Anwendungen.**

02 Vermeiden Sie leicht zu erratende Kombinationen wie Geburtstage, Namen oder allgemeine Phrasen.

03 Verwenden Sie einen seriösen Passwort-manager, um Ihre Passwörter sicher zu speichern und zu verwalten.

04 Aktualisieren Sie Ihre Passwörter regelmäßig und vermeiden Sie die Wiederverwendung alter Passwörter.

Seien Sie vorsichtig mit E-Mails und Anhängen!

01 **Überprüfen Sie die E-Mail-Adresse des Absenders, bevor Sie Anhänge öffnen oder auf Links klicken.**

02 Geben Sie keine vertraulichen Informationen per E-Mail weiter.

03 Verwenden Sie bei Bedarf Verschlüsselungstools für den Versand sensibler Daten per E-Mail.

04 Melden Sie verdächtige E-Mails an die IT-Abteilung unseres Unternehmens.

Halten Sie Software und Betriebssystem auf dem neuesten Stand!

01 **Halten Sie das Betriebssystem und den Virenscanner immer auf dem neusten Stand. Führen Sie Updates SOFORT aus.**

02 Suchen Sie regelmäßig nach Software-Updates und installieren Sie diese umgehend.

03 Aktivieren Sie nach Möglichkeit automatische Updates, um sicherzustellen, dass Ihr Gerät immer auf dem neuesten Stand ist.

04 Wenden Sie sich an Ihre IT-Abteilung, wenn Sie Schwierigkeiten mit den Updates haben oder Unterstützung benötigen.

Verwenden Sie sichere Wi-Fi-Verbindungen!

01 **Vermeiden Sie die Nutzung öffentlicher Wi-Fi-Netzwerke für arbeitsbezogene Aufgaben.**

02 Verbinden Sie sich nur mit sicheren, passwortgeschützten Wi-Fi-Netzwerken.

03 Verwenden Sie nach Möglichkeit ein virtuelles privates Netzwerk (VPN), um Ihre Verbindung zu sichern, wenn Sie aus der Ferne arbeiten.

Schützen Sie Ihr Gerät vor Malware und Viren!

01 Verwenden Sie eine seriöse Antiviren-Software und halten Sie sie auf dem neuesten Stand. **Antiviren-Software muss täglich aktualisiert werden.**

02 Aktivieren Sie Echtzeit-Scans, um Bedrohungen sofort zu erkennen und zu entfernen.

03 Wenn möglich, verwenden Sie ein Kabelschloss, um Ihr Notebook an einem Schreibtisch oder anderen festen Gegenständen zu befestigen.

04 Seien Sie vorsichtig beim Herunterladen von Dateien oder Anklicken von Links aus unbekannten Quellen.

05 Benachrichtigen Sie unsere IT-Abteilung umgehend, wenn Sie vermuten, dass Ihr Notebook kompromittiert worden ist oder der Virenscanner Fehlermeldungen anzeigt.

Achtung!

Lassen Sie Ihr mobiles Gerät NIE unbeaufsichtigt!

Wenn Sie diese einfachen Richtlinien befolgen, können Sie Ihr firmeneigenes Gerät und die darin enthaltenen wertvollen Daten schützen. Bleiben Sie stets wachsam und melden Sie verdächtige Aktivitäten oder Bedenken sofort der IT-Abteilung. Die sichere Verwendung von Notebooks oder Smartphones ist ein wichtiger Bestandteil der Datensicherheit und des Datenschutzes in Ihrem Unternehmen.