Richtlinie Umgang mit mobilen Datenträgern / Privatgeräten

Die hier genannten Anweisungen gelten für alle Mitarbeiter und Mitarbeiterinnen von ……

Für dienstlich verwendete Mobilgeräte / Datenträger gelten nachfolgend angeführte Punkte. Die Richtlinie hat den Zweck das Risiko des ungewollten Abflusses von Daten an Dritte zu minimieren. Es sollen so wenig dienstliche Daten wie nötig und möglich auf mobilen Geräten gespeichert werden. Diese Anweisung gilt auch für dienstlich genutzte Privatgeräte, sofern deren Verwendung von der Geschäftsführung genehmigt wurde.

Richtlinie für Notebooks
Für jedes Gerät gilt:

- Sperrung des Kennwort (nicht offen einsehbar hinterlegen, alle drei Monate ändern)
- Verschlüsselung der Festplatte vor allem wenn sensible Daten darauf gespeichert werden
- Das Gerät niemals entsperrt an Dritte weitergegeben werden
- Das Gerät stets sicher verwahren (z.B. nicht unbeaufsichtigt im geparkten Auto)
- Unbekannte Datenträger oder Geräte dürfen nicht an das Gerät angeschlossen werden (es
- könnte sich Spähsoftware, Trojaner oder andere Malware darauf befinden)
- Das Betriebssystem muss regelmäßig aktualisiert werden
- Mitarbeiter und Mitarbeiterinnen dürfen ohne Befugnis keine fremde Software auf ihren
- Computern installieren
- Bei Verdacht auf Virenbefall, Datenspionage oder andere sicherheitsgefährdende Umstände ist unverzüglich eine Meldung zu erstatten.

Richtlinien für Smartphones
Für jedes Gerät gilt:

- Sperrung des Geräts mit PIN oder Kennwort (nicht offen einsehbar hinterlegen, alle drei
- Monate das Passwort ändern)
- Das Gerät sollte niemals entsperrt an Dritte weitergegeben werden
- Das Gerät sollte stets sicher verwahrt werden (z.B. nicht unbeaufsichtigt im geparkten
- Auto)
- Nicht benötigte Funktionen sollten deaktiviert werden (z.B. Bluetooth, WIFI, etc.)
- Das Gerät nicht über USB-Anschluss an unbekannte Quellen anschließen
- Das System sollte regelmäßig aktualisiert werden
- Überprüfung der Berechtigung, die eine App bei Installation verlangt
- Die Verwendung eines Jailbreak oder Rooting ist verboten
- Keinerlei Daten in Cloud-Diensten speichern
- Mitarbeiter dürfen keine fremde Apps installieren
- Bei Verdacht auf Virenbefall, Datenspionage oder andere sicherheitsgefährdende Umstände
- ist unverzüglich eine Meldung zu erstatten.

Weitere Verpflichtungen
Sollte der Dienstnehmer sein mobiles Gerät (Notebook, Smartphone, Datenstick, etc.) verlieren oder sollte es gestohlen werden, so ist dies unverzüglich der Geschäftsführung oder dem Datenschutzmanager zu melden, da ein möglicher Data-Breach innerhalb von 72 Stunden an die Datenschutzbehörde gemeldet werden muss.
Weiters ist das Senden von unternehmensbezogenen Daten an eine private E-Mail-Adresse oder die sonstige Mitnahme von unternehmensbezogenen Daten auf mobilen Datenträgern oder Cloud-Diensten für den privaten Gebrauch **verboten** !

Mitarbeiterbestätigung Umgang mit Datenträgern / Privatgeräten

Hiermit bestätige ich, _____, geboren am __.__,____, die Richtlinien zum Thema Umgang mit Datenträgern / Privatgeräten gelesen zu haben und einzuhalten.
Mir ist bewusst, dass ich keinerlei unternehmensbezogenen Daten an private E-Mail-Adressen senden darf oder anderswertig für den privaten Gebrauch verwenden darf.
Bei Verlust oder Diebstahl eines mobilen Datenträgers (Notebook, Smartphone, etc.) muss ich unverzüglich eine Meldung erstatten.

_____ _____

Ort, Datum Unterschrift