Blumatix Intelligence GmbH | Schwarzstrasse 48 | 5020 Salzburg
T: +43 662 243410 | W: www.blumatix.com | @: office@blumatix.com

Richtlinie für Tele- Heimarbeitsplätze (externe)

Das Ziel der Richtlinie ist es, durch einheitliche Regelungen möglichen Sicherheitsrisiken im Bereich der Informationssicherheit in unserem Unternehmen entgegenzuwirken und alle MitarbeiterInnen und Lieferanten mit IT-sicherheitsrelevanten Themen am Heimarbeitsplatz (Homeoffice) vertraut zu machen.

Hierzu zählen besonders:

• Der zur Verarbeitung von Daten genutzte PC/Notebook ist in einem von den anderen Wohnungsräumen klar separierten Arbeitszimmer aufzustellen.

• Das Arbeitszimmer muss verschließbar sein.

• Der Bildschirm ist so zu positionieren, dass keine unbefugte Einsichtnahme (weder im Zuge des Betretens des betreffenden Arbeitszimmers noch durch Beobachtung durch etwaige Fenster) stattfinden kann.

• Auf datenschutzrelevanten Datenträgern darf nur in verschlüsselter Form abgespeichert werden.

• Unterlagen auf Papier müssen vernichtet werden, wenn der Zweck für die Aufbewahrung der nicht mehr gegeben ist. Die Vernichtung hat in einer Form zu erfolgen, mit welcher gewährleistet ist, dass relevanten Daten nicht durch Unbefugte gelesen werden können; z.B. mit einem Aktenvernichter.

• Sollten Unterlagen mit Daten, die dem Datengeheimnis unterliegen, am häuslichen Arbeitsplatz bearbeitet werden, dürfen diese außerhalb der Telearbeit ausschließlich in verschließbaren Behältnissen gelagert werden. Dies gilt auch für den Transport von Unterlagen zwischen Dienststelle und häuslichem Arbeitsplatz.

• Die mit Telearbeit betrauten Lieferanten haben für ihre betriebliche Tätigkeit im Home-Office ausschließlich den Web-Browser einzusetzen und dürfen keine PDF-Daten, Bilder oder Screenshots von Dokumenten lokal speichern.

• Auf dem PC/Notebook ist ein aktueller Virenscanner zu installieren.

• Die Zugangs- und Zugriffspassworte sind unter Einhaltung der Komplexitätsvorschriften nach 90 Tagen zu ändern.

• Die Bildschirmsperre wird bei einer fehlenden Aktivität von 5 Minuten automatisch aktiviert und darf nur gegen entsprechende Authentifizierung (Passworteingabe) aufgehoben werden.

• Im Übrigen verweisen wir auf unsere allgemeine IT-Sicherheitsrichtlinie.