tüv.tekit
TÜV SAARLAND GRUPPE

TÜV SAARLAND

# CHECKLISTE
# IT-Sicherheit im Home-Office
## für Arbeitnehmer

Dieses Dokument ist eine kostenlose Vorlage der TÜV Saarland Gruppe. Sie dürfen und sollten dieses Dokument an die Gegebenheiten und Bedürfnisse in Ihrem Unternehmen anpassen.

Bitte beachten Sie, dass die TÜV Saarland Gruppe keine Haftung für etwaige Fehler sowohl im Entwurf als auch im fertigen Dokument übernimmt.

Sollten Sie bei der Anpassung oder Umsetzung des Dokuments Fragen oder Probleme haben, können Sie gerne die Unterstützung unserer Experten in Anspruch nehmen:

**tekit Consult Bonn GmbH | TÜV Saarland Gruppe**

+49 228 60 88 9 - 0

info@tekit.tuev-saar.de

| Maßnahme | zwingend | angeraten |
|---|---|---|
| **PHYSISCHE SICHERHEIT** | | |
| Die Betriebsmittel (z. B. Notebooks, mobile Datenträger etc.) und Informationen des Unternehmens sind im Home-Office vor dem physischen Zugriff durch unberechtigte Dritte geschützt. Die im Home-Office genutzten Räume werden bei Verlassen verschlossen (Fenster und Türen). | X | |
| Der Bildschirm im Home-Office kann nicht von unberechtigten Dritten eingesehen werden. Dies ist z. B. dann relevant, wenn der Arbeitsplatz im Home-Office sich im Erdgeschoss befindet und man durch ein Fenster Kenntnis vom Inhalt den Bildschirm nehmen könnte. Gleiches gilt für die Arbeit in öffentlichen Bereichen. Ein probates Mittel in diesem Kontext können auch Bildschirmschutzfolien sein. | X | |
| Der Bildschirm wird beim Verlassen des Arbeitsplatzes gesperrt (Tastenkombination WINDOWS + L) und zusätzlich sperrt sich das System bei einer Inaktivität (von z. B. 10 min) automatisch. | X | |
| Beim Verlassen des Arbeitsplatzes im Home-Office werden dort keine Informationen zurückgelassen („clean-desk"). | X | |
| Wenn mobile Betriebsmittelt wie z. B. Notebooks transportiert werden, sind diese beim Transport nicht unbeaufsichtigt. Bei Flügen sind solche Geräte wenn möglich im Handgepäck mitzuführen und nicht aufzugeben. | X | |
| **DATENSICHERUNG UND DATENENTSORGUNG** | | |
| Durch die Arbeit im Home-Office werden mehr Daten außerhalb des Unternehmens verarbeitet. Damit es nicht zu Datenverlust kommen kann, müssen die lokal gespeicherten Daten (am besten täglich) auf zentralen Laufwerken des Unternehmens (z. B. Serverlaufwerke) gesichert. Bevorzugt sollten wichtige Daten überhaupt nicht lokal gespeichert, sondern direkt auf den Laufwerken des Unternehmens ablegen. | X | |
| Vertrauliche Informationen des Unternehmens in Papierform und auf Datenträgern dürfen nicht über den Hausmüll entsorgt werden. Sollte keine Möglichkeit zur sicheren Vernichtung bestehen (Shredder), sollten die Datenträger und Dokumente bei nächster Gelegenheit wieder mit in das Unternehmen zurücktransportiert und dort entsorgt bzw. vernichtet werden. | X | |

| Maßnahme | zwingend | angeraten |
|---|---|---|
| **BETRIEBSSICHERHEIT** | | |
| Sowohl auf dem Arbeitsrechner als auch auf den privaten Geräten im gleichen Netzwerk (z. B. im gleichen WLAN) ist ein aktueller Virenschutz installiert. Zwar darf nicht auf privater Hardware gearbeitet werden, jedoch können sich Viren und andere Malware über ein Netzwerk verbreiten. Aus diesem Grund ist neben dem Virenschutz auch auf allen Geräten auf einen aktuellen Patchlevel (z. B. durch Windows Update) zu achten, da Viren oftmals Schwachstellen ausnutzen die durch Nichteinspielen von Updates entstehen. | X | |
| Insoweit im Home-Office vom Mitarbeiter ein WLAN genutzt wird, muss dieses ausreichend geschützt sein. Zwingend ist hier auf jeden Fall eine Verschlüsselung (z. B. nach WPA3). Anzuraten sind zusätzlich das Verbergen der Kennung des WLAN-Netzwerks (Hidden SSID) sowie die Aktivierung einer MAC-Filterung, damit nur bekannte Geräte sich mit dem WLAN verbinden dürfen. | X | |
| Der WLAN Router sollte ausreichend gesichert sein. Zu solchen Sicherungs-maßnahmen zählen eine aktuelle Firmware und ein ausreichend starkes Passwort (mind. 8 Zeichen und Umlaute) zum Login auf dem Router. | | X |
| **Sicherer Remote-Zugriff** | | |
| Der Zugriff auf Firmenressourcen erfolgt ausschließlich per VPN-Verbindung, da ansonsten Informationen abgehört oder manipuliert werden können. | X | |
| Für die Arbeit im Home-Office sollte auf die Nutzung von öffentlichen WLAN-Zugängen verzichtet werden und stattdessen nur der eigene Internetzugang des Mitarbeiters genutzt werden. | | X |