?✓ Checkliste Endgerätekonfiguration ✓?

Für sicheres mobiles Arbeiten im Homeoffice

Beim Arbeiten im Homeoffice müssen vergleichbare Situationen wie bei der Arbeit an einem Büroarbeitsplatz am KIT geschaffen werden. Insofern gelten auch im Homeoffice die KIT- Regeln.

Die hier aufgeführten Sicherheitsmaßnahmen schützen Sie vor Missbrauch Ihres IT-Arbeitsplatzes und der von Ihnen verarbeiteten Daten. Die Maßnahmen tragen auch zur Absicherung Ihres Heimnetzwerks bei.

☐ **Betriebssystem aktuell** und **Sicherheitsupdates** automatisiert?

- Patchmanagement: Die Arbeitsplatzrechner werden regelmäßig mit Patches und Updates der Betriebssystem- und Anwendungssoftware versorgt (WSUS, OPSI, etc.).
- 👍 Update-Stand unter Windows 10 prüfen: Startmenü – Einstellungen – Update und Sicherheit.
- Client-Firewall aktivieren.

☐ **Virenscanner** eingerichtet und aktuell?

- Schutz vor Schadprogrammen: Die Geräte verfügen über einen adäquaten Virenschutz, der auch einen Schutz gegen Schadsoftware bietet.
- Virenschutz am KIT
  Dieser IT-Service bietet den Mitarbeiterinnen und Mitarbeitern des KIT einen zentral verwalteten und tagesaktuellen Virenschutz für Notebooks, Desktop-PCs und Server.

☐ Festplattenverschlüsselung eingerichtet?

- Datenverschlüsselung (Kryptographie): Daten auf mobilen Geräten sollen verschlüsselt werden. Dies gilt sowohl für aktive Geräte wie bspw. Notebooks, Smartphones, Tablets als auch für mobile Datenträger wie USB-Sticks oder mobile Festplatten.
- Festplattenverschlüsselung am KIT

☐ Fernzugriff über das virtuelle private Netzwerk (VPN) eingerichtet?

- VPN bietet einen Schutz vor Angriffen auf die Kommunikation bzw. über Kommunikationsschnittstellen:
- Netzwerksicherheit: Der Zugang zum Datennetz des KIT geschieht über den für mobiles Arbeiten bzw. Arbeiten im Homeoffice vorgesehenen VPN-Zugang.

☐ **Home-Verzeichnis, OE-Ablage**, **Remote-Desktop**: eingerichtet und zugreifbar?

- Datensparsamkeit auf den Arbeitsplatzrechnern: Daten werden auf den zentralen Datenspeicher der OE gehalten. Der Zugriff auf die Daten erfolgt über den dafür vorgesehenen VPN-Zugang. Wenn möglich werden Daten nicht lokal gespeichert.

- KIT-Datenablage (OE-Verzeichnis)
  Dieser Dienst stellt einer Organisationseinheit des KIT (OE) eine hochverfügbare und zentrale Datenablage zur Verfügung.
- Das persönliche Verzeichnis (\\sccfs-home.scc.kit.edu\home) ist eine hochverfügbare, zentrale Datenablage für persönliche Daten und Dokumente. Die Ablage steht allen KIT-Beschäftigten zur Verfügung, kann jedoch nicht für andere Nutzer freigegeben werden.
- Microsoft Remote Desktop Services (RDS)
  Bereitstellung serverbasierter Windows-Desktops mit installierter Standardsoftware für KIT-Beschäftigte.

☐ Individuell benötigte Anwendungen installiert und konfiguriert?

- Bereitstellung der individuell benötigten Arbeitsumgebung. Im Zweifelsfall Absprache mit dem IT-Beauftragten der OE.
- Anwendungen aktuell halten.

☐ Kommunikationsanwendungen installiert (MS Teams, ZOOM, BigBlueButton, Rainbow)?

- Ermöglicht die Video- und Sprachkommunikation mit Kollegen*innen.
- Installation von Google Chrome oder MS Edge als Browser für BigBlueButton bzw. Jitsi
- Rainbow ist eine Telefonie-Software (App oder Browseranwendung), mit der verschiedene Endgeräte zum Telefonieren genutzt werden können Das Bürotelefon muss bspw. nicht auf die private Festnetznummer weitergeleitet werden.

☐ E-Mail-Zertifikat vorhanden und installiert?

- Das SCC stellt für die sichere Kommunikation im Internet Zertifikate zur Verfügung. Nutzerzertifikate werden für die E-Mail-Signatur und -Verschlüsselung benötigt.

☐ Automatische Bildschirmsperre aktiv, ggf. für Blickschutz sorgen, keine Weitergabe an Dritte!

- 👍 Bildschirmsperre unter Windows 10 einrichten: Startmenü – Einstellungen – Personalisierung – Sperrbildschirm – Einstellungen für Bildschirmschoner.
- Hinweis: Die unbeaufsichtigte Weitergabe und Nutzung des Geräts an/durch Dritte ist – auch vorübergehend – nicht zulässig.

?✓ Checkliste – Einführung Endgerätenutzung ✓?

Diese Checkliste enthält wichtige Informationen, die sicherstellen, dass Nutzende alle Komponenten und Anwendungen richtig und sicher bedienen können.

☐ Dienstvereinbarung, Leitfaden, Hinweispapier…. für mobile Arbeit

- Im Intranet unter A-Z - Dienstvereinbarung zur Telearbeit und mobilen Arbeit am Karlsruher Institut für Technologie (KIT)

☐ Token für die Zwei-Faktor-Authentifizierung (2FA-Token) vorhanden und eingerichtet?

- Verschiedene Dienste am KIT haben erhöhte Anforderungen an die IT-Sicherheit, die über eine einfache Anmeldung mit Nutzername und Passwort hinausgehen also einen zweiten Faktor erfordern. Dazu gehören insbesondere die SAP-Anwendungen (z.B. ESS/MSS zur Zeiterfassung) und das Campus-Management-System, aber auch verschiedene VPN-Zugänge. Zwei-Faktor-Authentifizierung am KIT.

☐ Sicherheit im Heimnetz

- Updates für den DSL-/Kabelrouter einspielen → Bedienungsanleitung des Heimrouters beachten.
- Standard-Passwort des Routers ändern, möglichst mehr als 12 Zeichen
  Passwortrichtlinien am KIT
- Trennung des dienstlich genutzten WLAN-Zugangs von nicht dienstlicher Nutzung des WLAN-Zugangs – WLAN-Gastzugang für Homeschooling, Freunde, Bekannte, „Zocker-Rechner“, usw. einrichten

☐ Awareness-Materialien zur Informationssicherheit:

- Faltblätter, Handouts oder Poster zu Praxistipps IT-Sicherheit, Erkennen betrügerischer Nachrichten und Meldepflicht für IT-Sicherheitsvorfälle
- Erklärvideos
- Online-Schulung NoPhish

☐ Hinweise zum gesunden Arbeiten im HomeOffice:

- Gesundes Arbeiten im Homeoffice (MED)
- Checklisten der Deutsche Gesetzliche Unfallversicherung (DGUV):
  CHECK-UP Homeoffice – Kurzversion
  CHECK-UP Homeoffice – Langversion

- „Unterstützung für Körper, Geist und Seele“ (MED)

Bei Fragen wenden Sie sich an Ihre IT-Beauftragten in der Organisationseinheit oder an den SCC-Servicedesk → servicedesk@scc.kit.edu