

## Checkliste IT-Sicherheit am Heimarbeitsplatz

Durch die Corona-Pandemie wurde in den meisten Unternehmen auf ein mobiles Arbeiten bzw. Homeoffice umgestellt. Diese Umstellungen veranlassen eine Reihe an Regelungen und Maßnahmen, die im Vorfeld beachtet werden müssen.

Folgende Checkliste soll Sie dabei unterstützen, die technischen und organisatorischen Voraussetzungen für ein sicheres sowie produktives Homeoffice aller Mitarbeiterinnen und Mitarbeiter im Unternehmen zu schaffen.

*Hinweis: Diese Liste ist als Empfehlung zu betrachten. Die domeba distribution GmbH übernimmt keine Gewähr für die Aktualität, Vollständigkeit oder Richtigkeit der Checkliste.*

Hilfsmittel und Informationsmaterial
Bundesamt für Sicherheit in der Informationstechnik: Tipps für sicheres mobiles Arbeiten. 17.03.2020. <a href="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf?__blob=publicationFile&amp;v=4">https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf?__blob=publicationFile&amp;v=4</a> (Abruf 03.11.2020)
DGUV: Arbeiten im Homeoffice – nicht nur in der Zeit der SARS-CpV-2-Epidemie. 20.08.2020. <a href="https://publikationen.dguv.de/widgets/pdf/download/article/3925">https://publikationen.dguv.de/widgets/pdf/download/article/3925</a> (Abruf 04.11.2020)

Checkpoint: Regelung Homeoffice	bitte ankreuzen	
	ja	nein
Es wurde geregelt, welche Mitarbeiter im Homeoffice arbeiten und welche in der Institution anwesend sein müssen.	<input type="checkbox"/>	<input type="checkbox"/>
Es wurde geregelt, wie die Dokumentation der Arbeitszeiten erfolgt, welche Arbeitszeitregelungen gelten und wie Leistungen im Homeoffice kontrolliert werden.	<input type="checkbox"/>	<input type="checkbox"/>
Es wurde sichergestellt, dass die Mitarbeiter im Homeoffice ergonomisch arbeiten können. <i>(ergonomische Arbeitsplatzgestaltung, Nutzung der bereitgestellten Arbeitsmittel, ergonomische Sitzhaltung)</i>	<input type="checkbox"/>	<input type="checkbox"/>
Es wurde festgelegt, welche Informationen (auf Papier oder in IT-Systemen) außerhalb unserer Institution transportiert und bearbeitet werden dürfen.	<input type="checkbox"/>	<input type="checkbox"/>
Es wurde festgelegt, welche Schutzvorkehrungen bzw. Sicherheitsmaßnahmen dabei zu treffen sind.	<input type="checkbox"/>	<input type="checkbox"/>
Es wurde geregelt, welche Kommunikationsmöglichkeiten im Homeoffice unter welchen Rahmenbedingungen genutzt werden dürfen.	<input type="checkbox"/>	<input type="checkbox"/>
Die Mitarbeiter wurden bezüglich der durch die Arbeit im Homeoffice entstehenden Risiken sensibilisiert. <i>(bspw. durch den unangemessenen Umgang mit Informationen, dem unsachgemäßen Transport von Arbeitsmitteln oder durch eine unsichere Kommunikation)</i>	<input type="checkbox"/>	<input type="checkbox"/>
Die Mitarbeiter wurden für den Wert der ihnen anvertrauten Informationen sensibilisiert.	<input type="checkbox"/>	<input type="checkbox"/>

Checkpoint: IT und Sicherheit	bitte ankreuzen	
	ja	nein
Die Mitarbeiter verfügen über einen schnellen und leistungsfähigen Internetzugang.	<input type="checkbox"/>	<input type="checkbox"/>
Es wurde ein sicherer Remote-Zugriff eingerichtet.	<input type="checkbox"/>	<input type="checkbox"/>
Es stehen ausreichend VPN-Zugänge zur Verfügung.	<input type="checkbox"/>	<input type="checkbox"/>
Die tragbaren IT-Systeme und Datenträger wurden verschlüsselt.	<input type="checkbox"/>	<input type="checkbox"/>
Die IT-Systeme wurden gehärtet. <i>(Authentifizierung einrichten, Virenschutz prüfen, Sicherheits-Updates, Protokollierung aktivieren)</i>	<input type="checkbox"/>	<input type="checkbox"/>
Findet eine regelmäßige Datensicherung der lokal gespeicherten Daten statt?	<input type="checkbox"/>	<input type="checkbox"/>
Die Mitarbeiter sind darüber informiert, dass Verluste von mobilen Geräten bei den jeweiligen Ansprechpartnern sofort zu melden sind.	<input type="checkbox"/>	<input type="checkbox"/>
Den Mitarbeitern ist ein Ansprechpartner für Hard- und Softwareprobleme bekannt.	<input type="checkbox"/>	<input type="checkbox"/>
Es wurde geregelt, wie Mitarbeiter mit institutionsfremden IT-Systemen/Netzen arbeiten dürfen.	<input type="checkbox"/>	<input type="checkbox"/>
Die Mitarbeiter wurden darauf hingewiesen, welche Regelungen und Maßnahmen zum Einbruchs- und Zutrittsschutz im Homeoffice zu beachten sind. <i>(Sicherstellung, dass Unbefugte zu keiner Zeit auf dienstliche IT und Unterlagen zugreifen können)</i>	<input type="checkbox"/>	<input type="checkbox"/>
Die Mitarbeiter wurden darüber informiert, dass ausgediente und defekte Datenträger nach sensiblen Daten überprüft werden müssen, bevor sie weggeworfen werden.	<input type="checkbox"/>	<input type="checkbox"/>
Werden dienstliche Unterlagen oder Informationen mit erhöhtem Schutzbedarf bearbeitet? <i>(wenn ja, sollten erweiterte, hochwertige Schutzmaßnahmen eingerichtet werden)</i>	<input type="checkbox"/>	<input type="checkbox"/>
Es wurden eindeutige Kontaktstellen und Kommunikationswege festgelegt, die von den Mitarbeitern verifiziert werden können.	<input type="checkbox"/>	<input type="checkbox"/>
Die Mitarbeiter wurden auf die Gefahren von Phishing-Attacken hingewiesen.	<input type="checkbox"/>	<input type="checkbox"/>
Die Mitarbeiter wurden in die entsprechenden Sicherheitsmaßnahmen der Institution eingewiesen und wurden im Umgang mit diesen geschult.	<input type="checkbox"/>	<input type="checkbox"/>
Alle relevanten Sicherheitsmaßnahmen der Mitarbeiter wurden in der verpflichtenden Sicherheitsrichtlinie dokumentiert.	<input type="checkbox"/>	<input type="checkbox"/>