CHECKLISTE – SICHERHEIT IM HOME-OFFICE

Die wichtigsten Aspekte zur IT-Sicherheit am Remote-Arbeitsplatz

ID	AKTIVITÄT	STATUS		
I	**SICHERHEIT IM HOME-OFFICE UND AM REMOTE-ARBEITSPLATZ**			
01	Ist am Remote-Arbeitsplatz ein Basisschutz für die Netzwerkverbindung (z.B. Internet, LAN, WLAN) eingestellt und in Betrieb?	OK	KO	N/A
02	Ist am Remote-Arbeitsplatz ein erweiterter Schutz für die Netzwerkverbindung (z.B. Internet, LAN, WLAN) eingestellt und in Betrieb?	OK	KO	N/A
03	Steht eine stabile und mit ausreichender Bandbreite ausgestattete Internetverbindung zur Verfügung?	OK	KO	N/A
04	Werden die Daten auf einem verschlüsselten Gerät gespeichert (z.B. Notebook)?	OK	KO	N/A
05	Existiert ein Sicherheitskonzept bei Ihrem Unternehmen, das auch die Sicherheit am Remote-Arbeitsplatz (z.B. im Home-Office) berücksichtigt?	OK	KO	N/A
06	Werden die Sicherheitsmaßnahmen am Remote-Arbeitsplatz mit der zuständigen IT-Abteilung (oder dem verantwortlichen Bereich für IT-Sicherheit) abgestimmt?	OK	KO	N/A
07	Existiert in Ihrer Organisation ein ISMS und ein Prozess zur laufenden Verbesserung des ISMS der auch Remote-Arbeitsplätze berücksichtigt?	OK	KO	N/A
08	Existieren Vorgaben zur sicheren Verwendung von (speziell mobilen) Endnutzergeräten vor allem auch in Bezug auf deren Verwendung am Remote-Arbeitsplatz (z.B. im Home-Office, auf Flughäfen oder in Hotels)?	OK	KO	N/A
09	Sind in Ihrer Organisation laufende Risikoanalyseprozesse etabliert, um etwaige IT-Sicherheitsrisiken und deren Auswirkungen auf Vermögenswerte verlässlich und rechtzeitig zu identifizieren und berücksichtigen diese Prozesse auch das Risikoprofil auf unterschiedlichen Remote-Arbeitsplätzen?	OK	KO	N/A
10	Sind in Ihrer Organisation laufende Risikomanagementprozesse etabliert, über die die adäquate Adressierung identifizierter IT-Sicherheitsrisiken insbesondere am Remote-Arbeitsplatz berücksichtigen?	OK	KO	N/A
II	**TEAM-KOLLABORATION UND KOOPERATION**			
11	Existieren geeignete, dokumentierte Vorgaben für Mitarbeiter/innen, die deren Verhalten zur Verwendung von Kollaborationswerkzeugen am Remote-Arbeitsplatz zur Erhöhung der IT-Sicherheit regeln?	OK	KO	N/A
12	Werden Mitarbeiter/innen laufend in Bezug auf die Relevanz und die Einhaltung wichtiger und sie betreffender IT-Sicherheitsmaßnahmen im Hinblick auf Risiken bei Remote-Arbeitsplätzen geschult?	OK	KO	N/A
13	Existieren definierte und dokumentierte Vorgaben für den Einsatz von Kollaborationswerkzeugen zur digitalen Zusammenarbeit?	OK	KO	N/A
14	Existiert ein Konzept zur Kontrolle und zur Beschränkung des Zugriffs auf virtuelle Events (z.B. eingeschränkte Gruppen für Videokonferenzen)?	OK	KO	N/A
15	Existiert ein Konzept zum Einsatz von kryptographischen Methoden in Verbindung mit Kollaborationswerkzeugen?	OK	KO	N/A

16	Existiert ein Regelwerk für die Verwendung von Desk-Sharing für Videokonferenz-Werkzeuge?	OK	KO	N/A
III	**BUSINESS-CONTINUITY UND BACKUP**			
17	Existiert eine Sammlung relevanter Kontaktdaten und ist diese in digitaler sowie in Papierform vorhanden?	OK	KO	N/A
18	Existiert für Notfälle eine Backup-Internetleitung (z.B. Mobiler Hotspot via Smartphone oder eigener LTE/5G-Router mit eigener SIM-Karte)?	OK	KO	N/A
19	Sind verschlüsselte, externe Datenträger für regelmäßig durchzuführende Backups vorhanden, die physikalisch vom Primärgerät (z.B. Notebook) getrennt sind?	OK	KO	N/A
20	Gibt es ein Konzept, wie der Zugang zum Remote-Arbeitsplatz (z.B. Home-Office) auch bei Defekten (z.B. Schlüsseldienst vorab auswählen bevor ein Türschloss kaputt geht, oder Kontaktdaten des Herstellers der Wohnungstür vorbereiten) möglich ist?	OK	KO	N/A
21	In welcher Form sind Arbeitsplätze (z.B. via Desk-Sharing) am Firmenstandort verfügbar, damit Ausweichmöglichkeiten vorhanden sind?	OK	KO	N/A
22	Sind Remote-Arbeitsplätze so gestaltet, dass der sichere Betrieb und die sichere Verwendung von IT-Lösungen sichergestellt ist?	OK	KO	N/A
23	Existieren Vorgaben zur sicheren Verwendung von (speziell mobilen) Endnutzergeräten vor allem auch in Bezug ihre Verwendung außerhalb der Organisation?	OK	KO	N/A