

Checkliste für den sicheren PC-Einsatz

(im Stand-alone-Betrieb)

(1) Zugangskontrolle

Ja Nein Entfällt

			Wurde der Verschluss des Raumes nach Arbeitsende angeordnet?
			Wurde die Abschaltung des Gerätes nach Arbeitsende angeordnet?

(2) Zugriffskontrolle

Ja Nein Entfällt

			Wird die Verwendung von Boot-Passwort und Setup-Passwort maschinell erzwungen?
			Erfolgt der Einsatz spezifischer Zugriffsschutzsoftware (z. B. mit systemtechnischer Überwachung von Aufbau, Länge, Historie und Gültigkeitsdauer des Benutzerpasswortes)?
			Wird ein Bildschirmschoner mit Passwortschutz genutzt?
			Gelangen Chipkarten-/Magnetkartenleser zum Einsatz?
			Erfolgt die Verschlüsselung einzelner Dateien, von Verzeichnissen, Partitionen oder der ganzen Festplatte (bei besonders sensiblen Daten)?
			Werden mechanische Sperren (Tastaturschlösser, Laufwerksverriegelungen, Gehäuseverriegelungen usw.) verwendet?
			Ist der PC bei einem Anschluss an ein öffentliches Netz gegen unberechtigte Zugriffe von Außen gesichert?

(3) Datenträgerkontrolle

Ja Nein Entfällt

			Erfolgt ein gesicherter Datenträgereinsatz durch Vorgabe von Regelungen (z. B. bezüglich der zentralen Beschaffung, Beschriftung und Weitergabe)?
			Wurde die Entfernung aller Datenträger aus dem PC und aller Ausdrucke aus den angeschlossenen Druckern bei Arbeitsende angeordnet?
			Existiert die Möglichkeit einer zugriffssicheren Aufbewahrung von Wechselplatten, USB-Sticks und anderen Datenträgern?
			Ist die datenschutzgerechte Entsorgung der nicht mehr benötigten/defekten Datenträger gemäß DIN 32757 gewährleistet?

(4) Transportkontrolle

Ja Nein Entfällt

			Wurden Datenschutzmaßnahmen zur Verhinderung eines unbefugten Lesens, Kopierens , Veränderns oder Löschens bei der Übertragung personenbezogener über ein externes Netz ergriffen?
			Ist der datenschutzgerechte Transport von Datenträgern gewährleistet?

(5) Katastrophenvorsorge

Ja Nein Entfällt

			Erfolgt die Durchführung von regelmäßigen Datensicherungen nach dem Generationenprinzip oder als Differenzsicherungen?
			Wird ein Data Safe zur Datenträgeraufbewahrung verwendet?
			Besteht die Möglichkeit einer Auslagerung von Sicherungsdatenträgern in einem Katastrophenarchiv?
			Besteht die Möglichkeit des Einsatzes einer unterbrechungsfreien Stromversorgung mit Überspannungsschutz?
			Gelangt eine permanent aktivierte Virenschutzsoftware zum Einsatz?
			Wurde ein Konzept bezüglich notwendiger Backup- und sonstiger Katastrophenvorsorgemaßnahmen erstellt?

(6) Organisatorische Maßnahmen

Ja Nein Entfällt

			Ist die Möglichkeit der Protokollierung und einer zeitnahen (täglichen) Auswertung der Protokolle bei einzelstehenden PC gegeben, die von mehreren Anwendern benutzt werden?
			Ist eine Dokumentation der Konfiguration (Hardware und Software) vorhanden?
			Hat eine schriftliche Verpflichtung der Benutzer zur Einhaltung der Sicherheitsmaßnahmen stattgefunden?
			Erfolgt eine ausführliche und laufende Mitarbeiterweisung und -schulung?
			Wurde die Nutzung von nicht dienstlich bereitgestellter Soft- und Hardware verboten?
			Erfolgt eine regelmäßige Kontrolle des PC auf Manipulationen, Setup-Veränderungen und bezüglich des Einsatzes von Fremdsoftware?