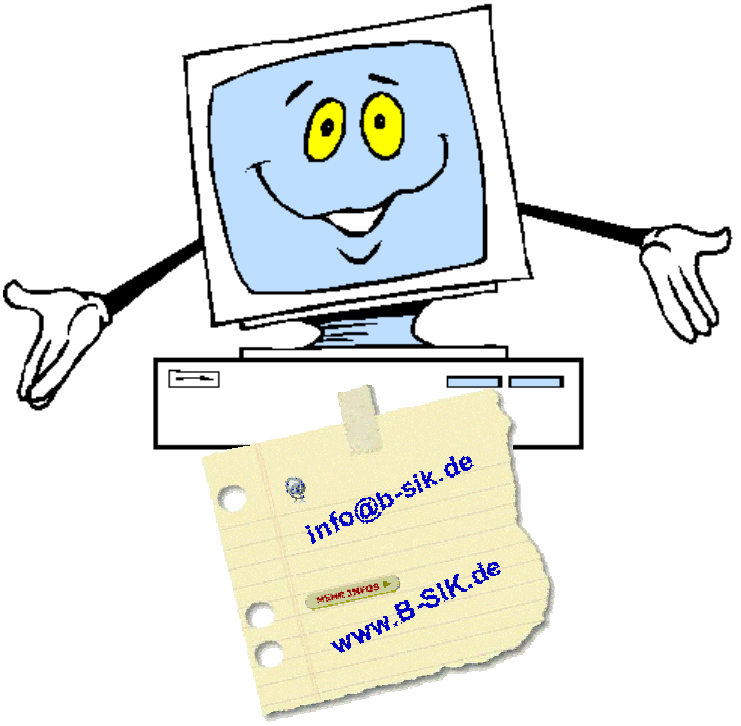
# EDV-Kurs

# Informationssicherheit




B-SIK

# Checkliste



## Informationssicherheitsmanagement

- ❑ Hat die Unternehmens- bzw. Behördenleitung die Informationssicherheitsziele festgelegt und sich zu ihrer Verantwortung für die Informationssicherheit bekannt? Sind alle gesetzlichen oder vertragsrechtlichen Gesichtspunkte berücksichtigt worden?
- ❑ Gibt es einen IT-Sicherheitsbeauftragten?
- ❑ Werden Sicherheitserfordernisse bei allen Projekten frühzeitig berücksichtigt (z. B. bei Planung eines neuen Netzes, Neuanschaffungen von IT-Systemen und Anwendungen, Outsourcing- und Dienstleistungsverträgen)?
- ❑ Besteht ein Überblick über die wichtigsten Anwendungen und IT-Systeme und deren Schutzbedarf?
- ❑ Gibt es einen Handlungsplan, der Sicherheitsziele priorisiert und die Umsetzung der beschlossenen Sicherheitsmaßnahmen regelt?
- ❑ Ist bei allen Sicherheitsmaßnahmen festgelegt, ob sie einmalig oder in regelmäßigen Intervallen ausgeführt werden müssen (z. B. Update des Viren-Schutzprogramms)?
- ❑ Sind für alle Sicherheitsmaßnahmen Zuständigkeiten und Verantwortlichkeiten festgelegt?
- ❑ Gibt es geeignete Vertretungsregelungen für Verantwortliche und sind die Vertreter mit ihren Aufgaben vertraut? Sind die wichtigsten Passwörter für Notfälle sicher hinterlegt?
- ❑ Sind die bestehenden Richtlinien und Zuständigkeiten allen Zielpersonen bekannt?
- ❑ Gibt es Checklisten, was beim Eintritt neuer Mitarbeiter und beim Austritt von Mitarbeitern zu beachten ist (Berechtigungen, Schlüssel, Unterweisung etc.)?
- ❑ Wird die Wirksamkeit von Sicherheitsmaßnahmen regelmäßig überprüft?
- ❑ Gibt es ein dokumentiertes Sicherheitskonzept?

## Sicherheit von IT-Systemen

- ❑ Werden vorhandene Schutzmechanismen in Anwendungen und Programmen genutzt?
- ❑ Werden flächendeckend Viren-Schutzprogramme eingesetzt?
- ❑ Sind allen Systembenutzern Rollen und Profile zugeordnet worden?
- ❑ Ist geregelt, auf welche Datenbestände jeder Mitarbeiter zugreifen darf? Gibt es sinnvolle Beschränkungen?
- ❑ Gibt es verschiedene Rollen und Profile für Administratoren oder darf jeder Administrator alles?
- ❑ Ist bekannt und geregelt, welche Privilegien und Rechte Programme haben?
- ❑ Werden sicherheitsrelevante Standardeinstellungen von Programmen und IT-Systemen geeignet angepasst oder wird der Auslieferungszustand beibehalten?
- ❑ Werden nicht benötigte sicherheitsrelevante Programme und Funktionen konsequent deinstalliert bzw. deaktiviert?
- ❑ Werden Handbücher und Produktdokumentationen frühzeitig gelesen?
- ❑ Werden ausführliche Installations- und Systemdokumentationen erstellt und regelmäßig aktualisiert?

# Checkliste



## Vernetzung und Internet-Anbindung

- ❑ Gibt es eine Firewall?
- ❑ Werden Konfiguration und Funktionsfähigkeit der Firewall regelmäßig kritisch überprüft und kontrolliert?
- ❑ Gibt es ein Konzept, welche Daten nach außen angeboten werden müssen?
- ❑ Ist festgelegt, wie mit gefährlichen Zusatzprogrammen (PlugIns) und aktiven Inhalten umgegangen wird?
- ❑ Sind alle unnötigen Dienste und Programmfunktionen deaktiviert?
- ❑ Sind Web-Browser und E-Mail-Programm sicher konfiguriert?
- ❑ Sind die Mitarbeiter ausreichend geschult?

## Beachtung von Sicherheitserfordernissen

- ❑ Werden vertrauliche Informationen und Datenträger sorgfältig aufbewahrt?
- ❑ Werden vertrauliche Informationen vor Wartungs- oder Reparaturarbeiten von Datenträgern oder IT-Systemen gelöscht?
- ❑ Werden Mitarbeiter regelmäßig in sicherheitsrelevanten Themen geschult?
- ❑ Gibt es Maßnahmen zur Erhöhung des Sicherheitsbewusstseins der Mitarbeiter?
- ❑ Werden bestehende Sicherheitsvorgaben kontrolliert und Verstöße geahndet?

## Wartung von IT-Systemen: Umgang mit Updates

- ❑ Werden Sicherheits-Updates regelmäßig eingespielt?
- ❑ Gibt es einen Verantwortlichen, der sich regelmäßig über Sicherheitseigenschaften der verwendeten Software und relevanter Sicherheits-Updates informiert?
- ❑ Gibt es ein Testkonzept für Softwareänderungen?

## Passwörter und Verschlüsselung

- ❑ Bieten Programme und Anwendungen Sicherheitsmechanismen wie Passwortschutz oder Verschlüsselung? Sind die Sicherheitsmechanismen aktiviert?
- ❑ Wurden voreingestellte oder leere Passwörter geändert?
- ❑ Sind alle Mitarbeiter in der Wahl sicherer Passwörter geschult?
- ❑ Werden Arbeitsplatzrechner bei Verlassen mit Bildschirmschoner und Kennwort gesichert?
- ❑ Werden vertrauliche Daten und besonders gefährdete Systeme wie Notebooks ausreichend durch Verschlüsselung oder andere Maßnahmen geschützt?

# Checkliste



## Notfallvorsorge

- ❑ Gibt es einen Notfallplan mit Anweisungen und Kontaktadressen?
- ❑ Werden alle notwendigen Notfallsituationen behandelt?
- ❑ Kennt jeder Mitarbeiter den Notfallplan und ist dieser gut zugänglich?

## Datensicherung

- ❑ Gibt es eine Backupstrategie?
- ❑ Ist festgelegt, welche Daten wie lange gesichert werden?
- ❑ Bezieht die Sicherung auch tragbare Computer und nicht vernetzte Systeme mit ein?
- ❑ Werden die Sicherungsbänder regelmäßig kontrolliert?
- ❑ Sind die Sicherungs- und Rücksicherungsverfahren dokumentiert?

## Infrastruktursicherheit

- ❑ Besteht ein angemessener Schutz der IT-Systeme gegen Feuer, Überhitzung, Wasserschäden, Überspannung und Stromausfall?
- ❑ Ist der Zutritt zu wichtigen IT-Systemen und Räumen geregelt? Müssen Besucher, Handwerker, Servicekräfte etc. begleitet bzw. beaufsichtigt werden?
- ❑ Besteht ein ausreichender Schutz vor Einbrechern?
- ❑ Ist der Bestand an Hard- und Software in einer Inventarliste erfasst?

Quelle: BSI: Leitfaden Informationssicherheit. IT-Grundschutz kompakt
https://www.bsi.bund.de/cae/servlet/contentblob/540280/publicationFile/34662/GS-Leitfaden_pdf.pdf