

Erstellt/geändert: <Datum>

Informationssicherheitsmanagement	Ja	Nein	Klärung
1. Hat die Unternehmensleitung die Informationssicherheitsziele festgelegt und sich zu ihrer Verantwortung für die Informationssicherheit bekannt? Sind alle gesetzlichen oder vertragsrechtlichen Gesichtspunkte berücksichtigt worden?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Gibt es einen IT-Sicherheitsbeauftragten?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. Werden Sicherheitserfordernisse bei allen Projekten frühzeitig berücksichtigt (z.B. bei Planung eines neuen Netzes, Neuanschaffungen von IT-Systemen und Anwendungen, Outsourcing- und Dienstleistungsverträgen)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. Besteht ein Überblick über die wichtigsten Anwendungen und IT-Systeme und deren Schutzbedarf?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. Gibt es einen Handlungsplan, der Sicherheitsziele priorisiert und die Umsetzung der beschlossenen Sicherungsmaßnahmen regelt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. Ist bei allen Sicherheitsmaßnahmen festgelegt, ob sie einmalig oder in regelmäßigen Intervallen ausgeführt werden müssen (z.B. Update des Viren-Schutzprogramms)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7. Sind für alle Sicherheitsmaßnahmen Zuständigkeiten und Verantwortlichkeiten festgelegt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8. Gibt es geeignete Vertretungsregelungen für Verantwortliche und sind die Vertreter mit ihren Aufgaben vertraut? Sind die wichtigsten Passwörter für Notfälle sicher hinterlegt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9. Sind die bestehenden Richtlinien und Zuständigkeiten allen Zielpersonen bekannt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10. Gibt es Checklisten, was beim Eintritt neuer Mitarbeiter und beim Austritt von Mitarbeitern zu beachten ist (Berechtigungen, Schlüssel, Unterweisungen etc.)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11. Wird die Wirksamkeit von Sicherheitsmaßnahmen regelmäßig überprüft?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12. Gibt es ein dokumentiertes Sicherheitskonzept?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sicherheit von IT-Systemen			
13. Werden vorhandene Schutzmechanismen in Anwendungen und Programmen genutzt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14. Werden flächendeckend Viren-Schutzprogramme eingesetzt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15. Sind allen Systembenutzern Rollen und Profile zugeordnet worden?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16. Ist geregelt, auf welche Datenbestände jeder Mitarbeiter zugreifen darf? Gibt es sinnvolle Beschränkungen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
17. Gibt es verschiedene Rollen und Profile für Administratoren oder darf jeder Administrator alles?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
18. Ist bekannt und geregelt, welche Privilegien und Rechte Programme haben?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
19. Werden sicherheitsrelevante Standardeinstellungen von Programmen und IT-Systemen geeignet angepasst oder wird der Auslieferungszustand beibehalten?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	Ja	Nein	Klärung
20. Werden nicht benötigte sicherheitsrelevante Programme und Funktionen konsequent deinstalliert bzw. deaktiviert?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
21. Werden Handbücher und Produktdokumentationen frühzeitig gelesen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
22. Werden ausführliche Installations- und Systemdokumentationen erstellt und regelmäßig aktualisiert?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vernetzung und Internet-Anbindung			
23. Gibt es eine Firewall?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
24. Werden Konfiguration und Funktionsfähigkeit regelmäßig kritisch überprüft und kontrolliert?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
25. Gibt es ein Konzept, welche Daten nach außen angeboten werden müssen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
26. Ist festgelegt, wie mit gefährlichen Zusatzprogrammen (PlugIns) und aktiven Inhalten umgegangen wird?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
27. Sind alle unnötigen Dienste und Programmfunktionen deaktiviert?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
28. Sind Web-Browser und E-Mail-Programm sicher konfiguriert?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
29. Sind die Mitarbeiter sicher geschult?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Beachtung von Sicherheitserfordernissen			
30. Werden vertrauliche Informationen und Datenträger sorgfältig aufbewahrt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
31. Werden vertrauliche Informationen vor Wartungs- oder Reparaturarbeiten von Datenträgern oder IT-Systemen gelöscht?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
32. Werden Mitarbeiter regelmäßig in sicherheitsrelevanten Themen geschult?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
33. Gibt es Maßnahmen zur Erhöhung des Sicherheitsbewusstseins der Mitarbeiter?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
34. Werden bestehenden Sicherheitsvorgaben kontrolliert und Verstöße geahndet?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wartung von IT-Systemen: Umgang mit Updates			
35. Werden Sicherheits-Updates regelmäßig eingespielt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
36. Gibt es einen Verantwortlichen, der sich regelmäßig über Sicherheitseigenschaften der verwendeten Software und relevanter Sicherheits-Updates informiert?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
37. Gibt es ein Testkonzept für Softwareänderungen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Prüfung und Wartung von IT-Systemen: Wartungsverträge			
38. Besteht die Möglichkeit der Einsichtnahme von personenbezogenen Daten bei den Prüfungs- oder Wartungsarbeiten durch den Dienstleister?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
39. Gibt es konforme Wartungsverträge gem. § 11 BDSG?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Passwörter und Verschlüsselung			
40. Bieten Programme und Anwendungen Sicherheitsmechanismen wie Passwortschutz oder Verschlüsselung? Sind die Sicherheitsmechanismen aktiviert?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	Ja	Nein	Klärung
41. Wurden voreingestellt oder leere Passwörter geändert?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
42. Sind alle Mitarbeiter in der Wahl sicherer Passwörter geschult?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
43. Werden Arbeitsplatzrechner bei Verlassen mit Bildschirmschoner und Kennwort gesichert?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
44. Werden vertrauliche Daten und besonders gefährdete Systeme wie Notebooks ausreichend durch Verschlüsselung oder andere Maßnahmen geschützt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Notfallvorsorge			
45. Gibt es einen Notfallplan mit Anweisungen und Kontaktadressen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
46. Werden alle notwendigen Notfallsituationen behandelt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
47. Kennt jeder Mitarbeiter den Notfallplan und ist dieser gut zugänglich?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Datensicherung			
48. Gibt es eine Backupstrategie?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
49. Ist festgelegt, welche Daten wie lange gesichert werden?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
50. Bezieht die Strategie auch tragbare Computer und nicht vernetzte Systeme mit ein?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
51. Werden die Sicherungsmedien regelmäßig kontrolliert?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
52. Sind die Sicherungs- und Rücksicherungsverfahren dokumentiert?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Infrastruktursicherheit			
53. Besteht ein angemessener Schutz der IT-Systeme gegen Feuer, Überhitzung, Wasserschäden, Überspannung und Stromausfall?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
54. Ist der Zutritt zu wichtigen IT-Systemen und Räumen geregelt? Müssen Besucher, Handwerker, Servicekräfte etc. begleitet bzw. beaufsichtigt werden?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
55. Besteht ein ausreichender Schutz vor Einbrechern?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
56. Ist der Bestand an Hard- und Software in einer Inventarliste erfasst?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Die Checkliste wurde in Anlehnung Leitfaden Informationssicherheit vom BSI erstellt und an die aktuellen Gegebenheiten angepasst.