*Bitte beachten Sie, dass es sich bei den hier veröffentlichten Mustertexten lediglich um allgemeine und beispielhafte Formulierungen handelt, die auf den jeweiligen Einzelfall noch individuell anzupassen sind. Wir können keine Haftung dafür übernehmen, dass der jeweilige Mustertext für den jeweils individuellen Sachverhalt uneingeschränkt verwendbar ist. Die unkritische Übernahme der Formulierungen erfolgt auf eigenes Risiko und ersetzt keineswegs die individuelle rechtliche Beratung.*

## <Firma>

# IT-Sicherheitsrichtlinie

## Einsatz und Nutzung der IT-Systeme -

**Inhaltsverzeichnis**

[Redaktionelle Vorbemerkung 4](#_Toc317933462)

[Präambel 4](#_Toc317933463)

[1 Allgemeine Regelungen 5](#_Toc317933464)

[1.1 IT-Sicherheitsbeauftragter 5](#_Toc317933465)

[1.2 Anwendungsbereich und Grundlagen für den Umgang mit IT-Systemen 5](#_Toc317933466)

1.2.1 Anwendungsbereich

[1.2.2 Zweckbindung der Systeme und Arbeitsmittel](#_Toc317933467)

[1.2.3 Tele- und Heimarbeitsplätze](#_Toc317933468)

[1.3 Einsatz und Freigabe von Datenverarbeitungsverfahren 6](#_Toc317933469)

[1.3.1 Sachlogische Prüfung](#_Toc317933470)

[1.3.2 Technische Testung](#_Toc317933471)

[1.3.3 Einrichtung der Verfahren](#_Toc317933472)

[1.3.4 Datenübernahme](#_Toc317933473)

[1.3.5 Freigabe zur Anwendung](#_Toc317933474)

[1.3.6 Aufbewahrung der Testergebnisse und der Dokumentationen](#_Toc317933475)

[1.4 Einsatz privater Hard- und Software/private Nutzung von betriebl. Geräten 8](#_Toc317933476)

[1.4.1 Einsatz privater Geräte](#_Toc317933477)

[1.4.2 Nutzung betrieblicher Geräte für private Zwecke](#_Toc317933478)

[1.5 Verwaltung und Administration der Datenverarbeitungsverfahren 9](#_Toc317933479)

[1.5.1 Verwaltung der Datenverarbeitungsverfahren](#_Toc317933480)

[1.5.2 Administrationsrechte](#_Toc317933481)

[1.5.3 Nachweis der Programmidentität](#_Toc317933482)

[1.5.4 Überwachung von Schnittstellen und Zugängen](#_Toc317933483)

[2 Nutzung von IT-Systemen 11](#_Toc317933484)

[2.1 Datensicherheit 11](#_Toc317933485)

[2.1.1 Allgemeine Grundsätze](#_Toc317933486)

[2.1.2 Verbindungen zu externen IT-Ressourcen](#_Toc317933487)

[2.1.3 Fremdrechner, Fremdunternehmen](#_Toc317933488)

[2.1.4 Wechseldatenträger](#_Toc317933489)

[2.1.5 Firewall und Internetschutz](#_Toc317933490)

[2.1.6 Schutz der Informationen vor unbefugter Kenntnisnahme](#_Toc317933491)

[2.1.7 Besucher](#_Toc317933492)

[2.1.8 Diebstahl und Verlust von Datenträgern](#_Toc317933493)

[2.1.9 Verhalten auf Reisen](#_Toc317933494)

[2.1.10 Arbeiten in fremden Umgebungen](#_Toc317933495)

[2.1.11 Meldung von Sicherheitsvorfällen und Verhalten bei Systemausfällen und Störungen](#_Toc317933496)

[2.2 Sicherungsmaßnahmen 17](#_Toc317933497)

[2.2.1 Sicherung von zentralen Datenbeständen](#_Toc317933498)

[2.2.2 Sicherung von lokalen Datenbeständen](#_Toc317933499)

[2.2.3 Protokollierung](#_Toc317933500)

[2.2.4 Verwendung von Passwörtern](#_Toc317933501)

[2.3 Einrichten und Verwalten von Benutzerkonten und Zugriffsrechten 22](#_Toc317933502)

[2.4 Verantwortlichkeit für Daten 23](#_Toc317933503)

[2.4.1 Ausscheiden, Umsetzung und Abwesenheit von Beschäftigten](#_Toc317933504)

[2.5 Computersicherheit, Computerviren und sonstige bösartige Software 23](#_Toc317933505)

[2.6 Notebooks und mobile Kommunikationsgeräte 24](#_Toc317933506)

[2.7 Weitergabe, Löschung und Entsorgung von Geräten und Datenträgern 25](#_Toc317933507)

[2.7.1 Weitergabe von elektronischen Datenträgern](#_Toc317933508)

[2.7.2 Löschung und Entsorgung von elektronischen Datenträgern](#_Toc317933509)

[3 E-Mail/Internet 27](#_Toc317933510)

[3.1 Gemeinsame Regelungen 27](#_Toc317933511)

[3.1.1 Private Nutzung von E-Mail und Internet](#_Toc317933512)

[3.1.2 Einweisung/Schulung](#_Toc317933513)

[3.1.3 Maßnahmen bei Verstößen](#_Toc317933514)

[3.2 Benutzung des E-Mail-Systems 28](#_Toc317933515)

[3.2.1 Zugangsbereitschaft](#_Toc317933516)

[3.2.2 Vertraulicher Versand von Daten und Informationen](#_Toc317933517)

[3.2.3 E-Mails als Geschäftsbriefe](#_Toc317933518)

[3.2.4 Rechtliche Verbindlichkeit von E-Mails](#_Toc317933519)

[3.2.5 Sonstige Verhaltensgrundsätze](#_Toc317933520)

[3.2.6 Spamfilterung](#_Toc317933521)

[3.3 Nutzung des Internetsystems 30](#_Toc317933522)

[3.3.1 Allgemeines](#_Toc317933523)

[3.3.2 Nutzung des Internetzugangs](#_Toc317933524)

[3.3.3 Allgemeine Sicherheitsregeln](#_Toc317933525)

[4 Protokollierung der E-Mail- und Internetnutzung 33](#_Toc317933526)

[5 Erklärung über die private Nutzung 35](#_Toc317933527)

[6 Überprüfung der Richtlinie „Informationssicherheit, Einsatz und Nutzung   
der IT-Systeme“ 36](#_Toc317933528)

**Anlage: Information und Erklärung zur privaten Nutzung der Kommunikationssysteme**

# 

*Redaktionelle Vorbemerkung*

*Die nachstehende Musterrichtlinie erhebt keinen Anspruch auf Vollständigkeit der möglichen Regelungen. Die Richtlinie ist aufgrund der unterschiedlichen technischen Umgebungen technik- und systemneutral und lediglich ein Leitfaden. Sie zeigt beispielhaft, welche Themen unter Datenschutzgesichtspunkten geregelt werden sollten, und gibt Beispiele für mögliche Regelungen, die aber i. d. R. nicht unverändert übernommen werden können, sondern an die individuellen Umstände im Unternehmen angepasst werden müssen. Umfang und Inhalt der Richtlinie sind auch davon abhängig, welche sonstigen Richtlinien und Dokumente im Unternehmen noch bestehen, z. B. Rechenzentrumsrichtlinie, Programmierrichtlinien, Notfallhandbuch oder Wiederanlaufplan. Ebenso sind Themen der allgemeinen Sicherheit hier nicht angesprochen und sollten in einer gesonderten Sicherheitsrichtlinie geregelt werden. Typische Regelungen in Betriebsvereinbarungen, z. B. zur E-Mail- und Internetnutzung, sollten hier nicht wiederholt werden, andererseits sollten bei fehlenden Betriebsvereinbarungen, z. B. weil kein Betriebsrat eingerichtet ist, Regelungen zum rechtskonformen Einsatz dieser Systeme getroffen werden. Inhaltlich können diese Regelungen an den Umfang und Regelungsinhalt von einschlägigen Betriebsvereinbarungen angelehnt werden.*

*Die IT-Sicherheit ist neben dem Einsatz, dem Betrieb und der Administration der IT-Systeme ein eigenständiges Thema. Es sollte deshalb im Unternehmen auch als solches definiert und gesondert adressiert werden. Als Rolle bietet sich die eines IT-Sicherheitsbeauftragten an. Der IT-Sicherheitsbeauftragte ist für den technischen Schutz der IT-Systeme und Anlagen verantwortlich und in Fragen der Datensicherheit Ansprechstelle des Datenschutzbeauftragten und der Revision. Die Bestellung, seine Aufgaben und Befugnisse sollten gesondert geregelt werden.*

*Präambel*

Die Datenverarbeitungssysteme einschließlich der gesamten IT-Infrastruktur (Server, Netzwerke, Arbeitsplatz-PCs etc.) und der Datenbestände zählen zur unternehmenskritischen Infrastruktur. Der Schutz dieser unternehmenskritischen IT-Infrastrukturen und Datenbestände gegen Bedrohungen aller Art, z. B. durch Schadsoftware wie Computerviren, Trojaner etc., Spionage, Missbrauch und Fehlbedienung, ist für das Unternehmen von großer Bedeutung. Es ist deshalb für das Unternehmen von großer Wichtigkeit, den sicheren und sachgemäßen Umgang mit allen Arten von Informationstechnologie zu regeln und damit das Unternehmen vor Schaden zu schützen. Diese Richtlinie trägt dazu bei, den erforderlichen Schutz zu gewährleisten und den Aufwand für den Schutz der Grundkriterien „Verfügbarkeit, Vertraulichkeit, Authentizität, Revisionsfähigkeit und Integrität“ zu optimieren.

Das gesamte, frei veränderbare Dokument erhalten Sie  
im Online-Fachportal **zum Sofort-Download**.  
Füllen Sie dazu jetzt das Formular auf der Webseite  
aus ([am Seitenende](https://fachportal-datenschutzbeauftragter.de/testen.php#testen)).

Bereits in der kostenlosen 4-Wochen-Testphase  
können Sie es **vollständig einsehen**  
und prüfen.

Um es uneingeschränkt zu nutzen,  
**wechseln** Sie **einfach** in einen  
kostenpflichtigen Account.  
[Hier Test-Zugang einrichten](https://fachportal-datenschutzbeauftragter.de/testen.php#testen)