Kapitel 5 – Vernetztes Zusammenarbeiten unter Nutzung digitaler Medien

Seite 5.1 Wertschätzende Zusammenarbeit

Prüfungsziel

Du sollst erklären können, wie Menschen im Betrieb respektvoll, verantwortungsvoll und wertschätzend zusammenarbeiten.

Für die Prüfung sind hier vor allem wichtig:

- wertschätzende Zusammenarbeit
- Interdisziplinarität
- Interkulturalität
- effektive Zusammenarbeit in verschiedenen Teams
- integres und respektvolles Verhalten
- gemeinsame Verantwortung für Zusammenarbeit
- Wertschätzung der Beiträge einzelner Teammitglieder
- Unternehmenswerte beachten
- betriebliche Ethikregeln anwenden
- gesellschaftliche Vielfalt bei betrieblichen Abläufen berücksichtigen

---

Was bedeutet wertschätzende Zusammenarbeit?

Wertschätzende Zusammenarbeit bedeutet, dass Menschen im Betrieb respektvoll miteinander umgehen und die Beiträge anderer anerkennen.

Einfach gesagt:

Man arbeitet nicht nur fachlich zusammen, sondern achtet auch darauf, wie man miteinander umgeht.

Wertschätzende Zusammenarbeit zeigt sich zum Beispiel durch:

- höfliche Kommunikation
- respektvollen Umgang
- Zuhören
- sachliche Kritik
- Hilfsbereitschaft
- Zuverlässigkeit
- Fairness
- Anerkennung der Arbeit anderer
- Rücksicht auf unterschiedliche Meinungen
- konstruktive Lösung von Konflikten

Warum ist wertschätzende Zusammenarbeit wichtig?

Gute Zusammenarbeit verbessert die Arbeitsqualität und das Betriebsklima.

Vorteile:

- weniger Konflikte
- bessere Kommunikation
- höhere Motivation
- bessere Teamleistung
- weniger Fehler durch Missverständnisse
- mehr Vertrauen im Team
- schnelleres Lösen von Problemen
- bessere Zusammenarbeit zwischen Abteilungen
- bessere Kundenbetreuung

Beispiel aus der IT:

Ein Support-Mitarbeiter, ein Netzwerkadministrator und ein Datenschutzbeauftragter müssen gemeinsam ein Problem lösen.

Wenn alle respektvoll kommunizieren und ihr Fachwissen einbringen, wird die Lösung schneller und besser gefunden.

Interdisziplinarität

Interdisziplinarität bedeutet, dass Menschen aus unterschiedlichen Fachbereichen zusammenarbeiten.

Einfach gesagt:

Verschiedene Fachrichtungen arbeiten gemeinsam an einer Aufgabe.

Beispiele im Betrieb:

Fachbereich	Beitrag
IT	technische Lösung planen und umsetzen
Datenschutz	personenbezogene Daten schützen
Einkauf	Angebote einholen und Bestellung durchführen
Buchhaltung	Kosten prüfen und Zahlungen bearbeiten
Personalabteilung	Mitarbeiterdaten und Schulungen verwalten
Geschäftsführung	Entscheidung und Verantwortung übernehmen
Fachabteilung	Anforderungen aus der Praxis liefern

Beispiel für interdisziplinäre Zusammenarbeit

Ein Unternehmen möchte ein neues Ticketsystem einführen.

Daran beteiligt sein können:

- IT-Abteilung
- Datenschutzbeauftragter
- Betriebsrat
- Einkauf
- Support-Team
- Geschäftsführung
- Fachabteilungen

Warum?

Das Ticketsystem betrifft nicht nur Technik.

Es betrifft auch:

- Arbeitsabläufe
- Datenschutz
- Kosten
- Benutzerfreundlichkeit
- Rechte und Rollen
- Auswertung von Daten
- Schulung der Mitarbeiter

Vorteile von Interdisziplinarität

- verschiedene Perspektiven werden berücksichtigt
- bessere Entscheidungen
- weniger blinde Flecken
- Fachwissen wird kombiniert
- Risiken werden früher erkannt
- Lösungen passen besser zum Betrieb

Mögliche Schwierigkeiten

- unterschiedliche Fachsprachen
- unterschiedliche Interessen
- Missverständnisse
- längere Abstimmungen
- Konflikte über Zuständigkeiten

Prüfungsnah:

Interdisziplinäre Zusammenarbeit ist wichtig, weil IT-Lösungen fast immer mehrere Bereiche eines Unternehmens betreffen.

Interkulturalität

Interkulturalität bedeutet, dass Menschen mit unterschiedlichen kulturellen Hintergründen zusammenarbeiten.

Einfach gesagt:

Menschen haben unterschiedliche Erfahrungen, Sprachen, Werte oder Kommunikationsgewohnheiten.

Im Betrieb sollte man damit respektvoll umgehen.

Beispiele für interkulturelle Unterschiede

Unterschiede können sich zeigen bei:

- Sprache
- Kommunikationsstil
- Höflichkeitsformen
- Umgang mit Kritik
- Umgang mit Hierarchien
- Zeitverständnis
- religiösen oder kulturellen Gewohnheiten
- Feiertagen
- Arbeits- und Gesprächsgewohnheiten

Wichtig:

Interkulturalität bedeutet nicht, Menschen in Schubladen zu stecken.

Es bedeutet, offen, respektvoll und aufmerksam mit Unterschieden umzugehen.

Warum ist Interkulturalität wichtig?

In vielen Betrieben arbeiten Menschen mit verschiedenen Hintergründen zusammen.

Auch Kunden, Lieferanten oder externe Dienstleister können international sein.

Vorteile:

- vielfältige Perspektiven
- bessere Ideen
- bessere Zusammenarbeit mit internationalen Kunden
- mehr Verständnis für unterschiedliche Nutzergruppen
- bessere Problemlösung durch verschiedene Erfahrungen

Mögliche Herausforderungen:

- Sprachbarrieren
- Missverständnisse
- unterschiedliche Erwartungen
- Unsicherheit im Umgang miteinander
- Vorurteile

Respektvolle Zusammenarbeit

Respektvolle Zusammenarbeit bedeutet, andere Menschen ernst zu nehmen und fair zu behandeln.

Respekt zeigt sich zum Beispiel durch:

- ausreden lassen
- sachlich bleiben
- keine Beleidigungen
- keine abwertenden Kommentare
- Kritik auf Verhalten oder Sache beziehen, nicht auf die Person
- Hilfe anbieten
- Vereinbarungen einhalten
- andere Meinungen anhören
- Fehler offen, aber fair ansprechen

Integres Verhalten

Integer bedeutet ehrlich, zuverlässig und verantwortungsbewusst.

Integres Verhalten im Betrieb bedeutet:

- ehrlich kommunizieren
- Fehler nicht vertuschen
- vertrauliche Informationen schützen
- Regeln einhalten
- keine falschen Versprechen machen
- Verantwortung übernehmen
- fair mit Kollegen, Kunden und Partnern umgehen

Beispiel:

Ein Auszubildender bemerkt, dass er versehentlich eine falsche Konfiguration gesetzt hat.

Integeres Verhalten wäre:

- Fehler melden
- bei der Behebung helfen
- daraus lernen
- nicht versuchen, den Fehler zu verstecken

Gemeinsame Verantwortung im Team

Gemeinsame Verantwortung bedeutet, dass nicht jeder nur „seinen kleinen Teil“ sieht, sondern das gemeinsame Ziel beachtet.

Beispiele:

- Informationen rechtzeitig weitergeben
- andere unterstützen
- Probleme nicht einfach weiterreichen
- Zuständigkeiten klären
- Ergebnisse gemeinsam prüfen
- auf Qualität achten
- bei Fehlern gemeinsam Lösungen suchen

Beispiel IT-Support:

Ein Ticket wird von Level 1 an Level 2 weitergegeben.

Wertschätzende Zusammenarbeit bedeutet:

- Problem sauber dokumentieren
- bisherige Schritte notieren
- keine Schuldzuweisungen
- Rückfragen beantworten
- gemeinsam Lösung finden

Wertschätzung der Beiträge jedes Teammitglieds

Jedes Teammitglied kann einen wichtigen Beitrag leisten.

Das gilt auch dann, wenn Personen unterschiedliche Rollen, Erfahrung oder Ausbildungsstände haben.

Beispiele:

- Azubi erkennt einen Fehler in der Dokumentation

- Support-Mitarbeiter kennt häufige Kundenprobleme
- Administrator kennt technische Abhängigkeiten
- Datenschutzbeauftragter erkennt rechtliche Risiken
- Fachabteilung kennt den echten Arbeitsablauf
- Einkauf kennt Lieferzeiten und Vertragsbedingungen

Wichtig:

Gute Teams nutzen unterschiedliche Stärken.

Unternehmenswerte

Unternehmenswerte sind Grundsätze, nach denen ein Unternehmen handeln möchte.

Beispiele:

- Kundenorientierung
- Qualität
- Zuverlässigkeit
- Respekt
- Nachhaltigkeit
- Datenschutz
- Sicherheit
- Transparenz
- Fairness
- Innovation
- Verantwortung

Wichtig für die Prüfung:

Beschäftigte sollen Unternehmenswerte im Arbeitsalltag beachten.

Beispiel:

Wenn ein Unternehmen Datenschutz als wichtigen Wert nennt, müssen Beschäftigte sorgfältig mit Kundendaten umgehen.

Betriebliche Ethikregeln

Betriebliche Ethikregeln beschreiben, welches Verhalten im Unternehmen als richtig und verantwortungsvoll gilt.

Beispiele:

- keine Diskriminierung
- respektvoller Umgang

- keine Korruption
- keine privaten Vorteile durch dienstliche Entscheidungen
- vertrauliche Informationen schützen
- fairer Umgang mit Kunden
- sachliche Kommunikation
- keine Manipulation von Daten
- verantwortungsvoller Umgang mit IT-Systemen

Wertschätzung gesellschaftlicher Vielfalt

Gesellschaftliche Vielfalt bedeutet, dass Menschen unterschiedlich sind.

Unterschiede können zum Beispiel betreffen:

- Alter
- Geschlecht
- Sprache
- Herkunft
- Kultur
- Religion
- Behinderung
- Erfahrung
- Bildungsweg
- Lebenssituation
- Arbeitsweise

Wichtig:

Im Betrieb sollen Menschen fair und respektvoll behandelt werden.

Bei betrieblichen Abläufen soll Vielfalt berücksichtigt werden.

Beispiel: Vielfalt bei IT-Lösungen berücksichtigen

Eine neue interne Software wird eingeführt.

Dabei sollte man beachten:

- Ist die Sprache verständlich?
- Ist die Bedienung barrierearm?
- Sind Rollen und Rechte fair geregelt?
- Werden verschiedene Arbeitsweisen berücksichtigt?
- Gibt es Schulungen für unterschiedliche Vorkenntnisse?
- Können auch neue Mitarbeiter oder Azubis das System verstehen?

Konflikte im Team

Konflikte können entstehen, wenn Menschen unterschiedliche Meinungen, Interessen oder Arbeitsweisen haben.

Typische Ursachen:

- unklare Zuständigkeiten
- schlechte Kommunikation
- Zeitdruck
- Missverständnisse
- unterschiedliche Erwartungen
- unfaire Aufgabenverteilung
- fehlende Informationen
- respektloser Umgang

Konstruktiver Umgang mit Konflikten

Bei Konflikten sollte man sachlich bleiben.

Sinnvolles Vorgehen:

```
Problem sachlich beschreiben
→ eigene Sicht erklären
→ andere Sicht anhören
→ gemeinsame Interessen suchen
→ Lösungsvorschläge sammeln
→ Vereinbarung treffen
→ Ergebnis prüfen
```

Wichtig:

Kritik sollte sich auf das Verhalten oder die Sache beziehen, nicht auf die Person.

Digitale Zusammenarbeit und Wertschätzung

Auch in digitalen Medien muss wertschätzend kommuniziert werden.

Beispiele:

- höfliche E-Mails schreiben
- keine abwertenden Kommentare im Chat
- klare Betreffzeilen nutzen
- Missverständnisse vermeiden
- Empfänger passend auswählen

- nicht unnötig alle in CC setzen
- keine vertraulichen Inhalte unbedacht teilen
- in Videokonferenzen ausreden lassen
- unterschiedliche Zeitzonen oder Arbeitszeiten beachten

Typische Fehler bei digitaler Zusammenarbeit

Fehler	Warum problematisch?
unhöfliche E-Mail	kann Konflikte auslösen
unklare Nachricht	führt zu Missverständnissen
falsche Adressatenliste	Datenschutz- oder Vertraulichkeitsproblem
keine Dokumentation	Wissen geht verloren
Schuldzuweisungen im Chat	schadet Teamklima
wichtige Infos nur mündlich	andere Teammitglieder werden ausgeschlossen
zu viele Personen in CC	Informationsflut und Datenschutzrisiko

---

Bezug zur Prüfung

In der Prüfung können Situationen beschrieben werden, bei denen du wertschätzendes oder problematisches Verhalten erkennen sollst.

Typische Aufgaben können sein:

- gutes Teamverhalten auswählen
- respektlose Kommunikation erkennen
- Interdisziplinarität erklären
- Interkulturalität einordnen
- Unternehmenswerte auf eine Situation anwenden
- gemeinsame Verantwortung im Team beschreiben
- ethische Regeln im Betrieb beurteilen
- digitale Kommunikation bewerten

Typische Prüfungsfrage 1

Was bedeutet wertschätzende Zusammenarbeit?

Antwort anzeigen

Wertschätzende Zusammenarbeit bedeutet, respektvoll miteinander umzugehen, Beiträge anderer anzuerkennen, sachlich zu kommunizieren und gemeinsam Verantwortung für gute

Zusammenarbeit zu übernehmen.

Typische Prüfungsfrage 2

Was bedeutet Interdisziplinarität?

Antwort anzeigen

Interdisziplinarität bedeutet, dass Menschen aus unterschiedlichen Fachbereichen zusammenarbeiten und ihr Fachwissen gemeinsam in eine Aufgabe einbringen.

Typische Prüfungsfrage 3

Nenne ein Beispiel für interdisziplinäre Zusammenarbeit in der IT.

Antwort anzeigen

Bei der Einführung eines Ticketsystems arbeiten zum Beispiel IT, Datenschutz, Betriebsrat, Einkauf, Support-Team und Fachabteilungen zusammen.

Typische Prüfungsfrage 4

Was bedeutet Interkulturalität?

Antwort anzeigen

Interkulturalität bedeutet, dass Menschen mit unterschiedlichen kulturellen Hintergründen zusammenarbeiten und dabei respektvoll mit unterschiedlichen Erfahrungen, Werten und Kommunikationsweisen umgehen.

Typische Prüfungsfrage 5

Was bedeutet integres Verhalten?

Antwort anzeigen

Integeres Verhalten bedeutet ehrlich, zuverlässig und verantwortungsbewusst zu handeln, Regeln einzuhalten und Fehler nicht zu vertuschen.

Typische Prüfungsfrage 6

Warum ist gemeinsame Verantwortung im Team wichtig?

Antwort anzeigen

Weil Teamarbeit nur funktioniert, wenn Informationen weitergegeben werden, Aufgaben abgestimmt sind und alle gemeinsam auf Qualität und Lösung des Problems achten.

Typische Prüfungsfrage 7

Nenne drei Beispiele für Unternehmenswerte.

Antwort anzeigen

Beispiele sind Kundenorientierung, Qualität, Zuverlässigkeit, Respekt, Nachhaltigkeit, Datenschutz, Sicherheit, Transparenz und Fairness.

Typische Prüfungsfrage 8

Was sind betriebliche Ethikregeln?

Antwort anzeigen

Betriebliche Ethikregeln beschreiben, welches Verhalten im Unternehmen als richtig und verantwortungsvoll gilt, zum Beispiel respektvoller Umgang, Datenschutz, Fairness und keine Diskriminierung.

Typische Prüfungsfrage 9

Warum sollte man die Beiträge jedes Teammitglieds wertschätzen?

Antwort anzeigen

Weil jedes Teammitglied durch seine Rolle, Erfahrung oder Perspektive zur Lösung beitragen kann. Gute Teams nutzen unterschiedliche Stärken.

Typische Prüfungsfrage 10

Nenne ein Beispiel für wertschätzende digitale Kommunikation.

Antwort anzeigen

Eine höfliche, klare E-Mail mit passender Betreffzeile, richtigen Empfängern und sachlichem Inhalt ist ein Beispiel für wertschätzende digitale Kommunikation.

Merksatz

- Wertschätzende Zusammenarbeit = respektvoll, fair, sachlich und verantwortungsvoll zusammenarbeiten
- Interdisziplinarität = Zusammenarbeit verschiedener Fachbereiche
- Interkulturalität = respektvoller Umgang mit unterschiedlichen kulturellen Hintergründen
- Integer handeln = ehrlich, zuverlässig und verantwortungsbewusst handeln
- Gute Teamarbeit bedeutet gemeinsame Verantwortung
- Unternehmenswerte und Ethikregeln müssen im Arbeitsalltag beachtet werden
- Vielfalt im Betrieb soll respektiert und bei Abläufen berücksichtigt werden
- Digitale Kommunikation muss genauso respektvoll sein wie persönliche Kommunikation

Seite 5.2 Verantwortungsbewusster Umgang mit digitalen Medien

Prüfungsziel

Du sollst erklären können, wie man digitale Medien im Betrieb verantwortungsvoll nutzt und dabei Persönlichkeitsrechte, Datenschutz und die Wirkung des eigenen Kommunikationsverhaltens beachtet.

Für die Prüfung sind hier vor allem wichtig:

- verantwortungsvoller Umgang mit digitalen Medien
- Zusammenarbeit im virtuellen Raum
- Wahrung der Persönlichkeitsrechte Dritter
- Speicherung digitaler Inhalte
- Darstellung digitaler Inhalte
- Weitergabe digitaler Inhalte
- Auswirkungen des eigenen Kommunikationsverhaltens
- Auswirkungen des eigenen Informationsverhaltens
- respektvolle digitale Kommunikation
- bewusster Umgang mit Informationen

Was sind digitale Medien?

Digitale Medien sind elektronische Medien, mit denen Informationen erstellt, gespeichert, übertragen oder ausgetauscht werden.

Beispiele:

- E-Mail
- Chat
- Ticketsystem
- Videokonferenz
- Cloudspeicher
- Messenger
- Intranet
- Wiki
- Lernplattform
- Social Media
- Projektmanagement-Tools
- digitale Dokumente
- Screenshots
- Fotos

- Videos
- geteilte Kalender

Was bedeutet verantwortungsvoller Umgang mit digitalen Medien?

Verantwortungsvoller Umgang bedeutet, digitale Medien bewusst, sicher, respektvoll und rechtlich korrekt zu nutzen.

Einfach gesagt:

Nicht alles, was technisch möglich ist, ist auch erlaubt oder sinnvoll.

Man muss beachten:

- Welche Informationen teile ich?
- Mit wem teile ich sie?
- Darf ich diese Information weitergeben?
- Sind personenbezogene Daten enthalten?
- Könnte jemand dadurch geschädigt werden?
- Ist der Ton respektvoll?
- Ist der Empfängerkreis richtig?
- Ist die Information vertraulich?
- Ist die Quelle zuverlässig?

Warum ist das im Betrieb wichtig?

Digitale Kommunikation ist schnell, aber Fehler verbreiten sich ebenfalls schnell.

Mögliche Risiken:

- vertrauliche Daten werden an falsche Personen gesendet
- personenbezogene Daten werden unzulässig geteilt
- Missverständnisse durch unklare Nachrichten
- Imageschaden durch unbedachte Äußerungen
- Konflikte durch unhöfliche Kommunikation
- Datenschutzverstöße
- Sicherheitsrisiken
- falsche Informationen verbreiten sich
- Persönlichkeitsrechte werden verletzt

Persönlichkeitsrechte Dritter

Persönlichkeitsrechte schützen die Würde, Privatsphäre und persönliche Entfaltung von Menschen.

Im Betrieb bedeutet das:

Man darf andere Personen nicht ohne Grund bloßstellen, überwachen, beleidigen, fotografieren, filmen oder personenbezogene Informationen verbreiten.

Beispiele für geschützte Informationen:

- Name
- Adresse
- Telefonnummer
- E-Mail-Adresse
- Geburtsdatum
- Foto
- Video
- Gesundheitsdaten
- Leistungsdaten
- Personalakte
- private Nachrichten
- Standortdaten
- Bewertungen über eine Person

Beispiele für Verletzungen von Persönlichkeitsrechten

Situation	Problem
Foto eines Kollegen ohne Zustimmung im Intranet hochladen	Recht am eigenen Bild verletzt
Screenshot mit Kundendaten im Chat teilen	Datenschutzproblem
private Information über Kollegen weiterleiten	Verletzung der Privatsphäre
abwertender Kommentar über Mitarbeiter im Gruppenchat	respektlos und möglicherweise rechtlich problematisch
ungefragtes Aufzeichnen einer Videokonferenz	Persönlichkeitsrechte und Datenschutz betroffen
Leistungsdaten öffentlich im Team posten	Bloßstellung und Datenschutzrisiko

---

Recht am eigenen Bild

Das Recht am eigenen Bild bedeutet, dass Menschen grundsätzlich selbst entscheiden dürfen, ob Bilder von ihnen veröffentlicht oder verbreitet werden.

Prüfungsnah:

Ein Foto von Kollegen, Kunden oder Besuchern sollte nicht einfach ohne Zustimmung veröffentlicht oder weitergegeben werden.

Beispiel:

Ein Azubi macht ein Foto vom Team und lädt es ohne Nachfrage in eine öffentliche Social-Media-Gruppe hoch.

Das ist problematisch, weil die abgebildeten Personen nicht zugestimmt haben.

Speichern digitaler Inhalte

Beim Speichern digitaler Inhalte muss geprüft werden, ob die Speicherung notwendig, erlaubt und sicher ist.

Beispiele für digitale Inhalte:

- Kundendaten
- Mitarbeiterdaten
- Tickets
- Chatverläufe
- E-Mails
- Screenshots
- Logs
- Fotos
- Dokumente
- Vertragsdaten
- Projektdaten

Wichtige Fragen:

- Darf ich diese Daten speichern?
- Gibt es einen betrieblichen Zweck?
- Sind personenbezogene Daten enthalten?
- Wo werden die Daten gespeichert?
- Wer hat Zugriff?
- Wie lange werden die Daten benötigt?
- Müssen Daten gelöscht werden?
- Ist die Speicherung sicher?

Darstellung digitaler Inhalte

Darstellung bedeutet, wie Inhalte angezeigt oder präsentiert werden.

Beispiele:

- Bildschirmfreigabe in Videokonferenz
- Präsentation
- Dashboard
- Monitoring-Anzeige

- Ticketübersicht
- Chatnachricht
- Screenshot
- Wiki-Seite
- Intranet-Beitrag

Risiken bei der Darstellung:

- vertrauliche Daten sind sichtbar
- falsche Personen sehen Kundendaten
- private Nachrichten werden versehentlich gezeigt
- Passwörter oder Tokens sind sichtbar
- personenbezogene Daten werden unnötig angezeigt
- sensible Tickets werden im Meeting geteilt

Beispiel: Bildschirmfreigabe

Ein Mitarbeiter teilt in einer Videokonferenz seinen Bildschirm.

Auf dem Desktop sind sichtbar:

- private E-Mails
- Kundendaten
- interne Tickets
- Zugangsdaten in einer Datei
- Chatnachrichten

Richtiges Verhalten:

- nur das benötigte Fenster teilen
- sensible Tabs schließen
- Benachrichtigungen deaktivieren
- keine Passwörter sichtbar lassen
- vor der Freigabe prüfen, was zu sehen ist

Weitergabe digitaler Inhalte

Weitergabe bedeutet, dass Informationen an andere Personen oder Stellen übermittelt werden.

Beispiele:

- E-Mail weiterleiten
- Datei in Cloud teilen
- Screenshot senden
- Link freigeben

- Chatnachricht kopieren
- Dokument exportieren
- Daten an Dienstleister senden
- Logdatei an Support weitergeben

Wichtige Fragen vor der Weitergabe:

- Ist die Weitergabe erlaubt?
- Ist der Empfänger berechtigt?
- Sind personenbezogene Daten enthalten?
- Ist die Datei wirklich notwendig?
- Müssen Daten anonymisiert werden?
- Ist der Übertragungsweg sicher?
- Ist der Empfängerkreis zu groß?
- Gibt es vertrauliche Informationen?

Empfängerkreis prüfen

Ein häufiger Fehler ist, Informationen an zu viele oder falsche Personen zu senden.

Beispiele:

Fehler	Risiko
„Allen antworten“ ohne Prüfung	zu viele Personen erhalten Informationen
falsche E-Mail-Adresse	Daten gehen an falschen Empfänger
offene Verteilerliste	E-Mail-Adressen werden sichtbar
Cloud-Link öffentlich freigegeben	unberechtigte Personen können zugreifen
Screenshot in Gruppenchat	sensible Informationen erreichen falsche Personen

---

Kommunikationsverhalten

Kommunikationsverhalten beschreibt, wie jemand Informationen austauscht.

Gutes Kommunikationsverhalten ist:

- sachlich
- höflich
- verständlich
- zielgerichtet
- respektvoll
- vollständig genug
- nicht unnötig lang
- empfängerorientiert

- datenschutzbewusst
- sicherheitsbewusst

Schlechtes Kommunikationsverhalten

Schlechtes Kommunikationsverhalten kann Konflikte oder Schäden verursachen.

Beispiele:

- unhöfliche Nachrichten
- unklare Anweisungen
- Schuldzuweisungen im Chat
- vertrauliche Informationen in offenen Kanälen
- unnötig viele Personen in CC
- private Kritik in öffentlicher Gruppe
- Weiterleitung ohne Prüfung
- vorschnelles Teilen unbestätigter Informationen
- Screenshots mit sichtbaren Kundendaten

Informationsverhalten

Informationsverhalten beschreibt, wie jemand Informationen sucht, bewertet, speichert, nutzt und weitergibt.

Gutes Informationsverhalten bedeutet:

- Quellen prüfen
- Informationen nicht ungeprüft weitergeben
- vertrauliche Informationen schützen
- nur notwendige Daten speichern
- Informationen aktuell halten
- klare Ablage nutzen
- Daten nicht unnötig vervielfältigen
- falsche Informationen korrigieren
- Berechtigungen beachten

Beispiel: Falsche Information im Betrieb

Ein Mitarbeiter liest in einem Chat, dass ein System angeblich ausgefallen ist.

Er informiert sofort mehrere Kunden, ohne die Information zu prüfen.

Später stellt sich heraus, dass es nur ein lokales Problem war.

Problem:

- unnötige Unruhe
- Vertrauensverlust
- zusätzliche Arbeit
- falsche Kommunikation
- schlechter Eindruck beim Kunden

Richtiges Verhalten:

Erst prüfen, dann gezielt informieren.

Zusammenarbeit im virtuellen Raum

Virtueller Raum bedeutet digitale Zusammenarbeit ohne gemeinsamen physischen Ort.

Beispiele:

- Videokonferenz
- Chat
- Cloud-Dokument
- Ticketsystem
- Remote-Support
- Online-Schulung
- gemeinsames Wiki
- Projektmanagement-Tool

Regeln für gute virtuelle Zusammenarbeit

- pünktlich an Meetings teilnehmen
- Mikrofon stummschalten, wenn man nicht spricht
- andere ausreden lassen
- klare Beiträge schreiben
- Aufgaben dokumentieren
- Zuständigkeiten festhalten
- Entscheidungen nachvollziehbar speichern
- vertrauliche Informationen schützen
- passende Kanäle nutzen
- nicht in zu vielen parallelen Chats arbeiten
- Datenschutz beachten

Digitale Inhalte und Dauerhaftigkeit

Digitale Inhalte können lange gespeichert, kopiert und weitergeleitet werden.

Wichtig:

Was einmal digital geteilt wurde, lässt sich oft schwer vollständig zurückholen.

Beispiele:

- weitergeleitete Screenshots
- exportierte Chatverläufe
- heruntergeladene Dateien
- E-Mail-Anhänge
- öffentliche Social-Media-Beiträge
- geteilte Cloud-Links

Prüfungsnah:

Vor dem Teilen überlegen, ob Inhalt, Empfänger und Zweck passen.

Umgang mit Screenshots

Screenshots sind im IT-Bereich nützlich, aber riskant.

Nützlich für:

- Fehlermeldungen
- Dokumentation
- Supportfälle
- Schulungsunterlagen
- Beweise für Systemzustände

Risiken:

- Kundendaten sichtbar
- personenbezogene Daten sichtbar
- interne Systeme sichtbar
- IP-Adressen oder Hostnamen sichtbar
- Zugangsdaten sichtbar
- vertrauliche Tickets sichtbar

Richtiges Verhalten:

- sensible Daten schwärzen
- nur nötigen Bildausschnitt verwenden
- Empfänger prüfen
- Screenshot sicher speichern
- Screenshot löschen, wenn nicht mehr benötigt

Umgang mit Links und Freigaben

Cloud-Links und Datei-Freigaben müssen vorsichtig genutzt werden.

Risiken:

- Link ist öffentlich erreichbar
- falsche Berechtigung
- Bearbeitungsrechte statt Leserechte
- Link wird weitergeleitet
- Ablaufdatum fehlt
- Datei enthält sensible Daten

Sichere Maßnahmen:

- Empfänger gezielt festlegen
- nur notwendige Rechte vergeben
- Ablaufdatum setzen, wenn möglich
- Passwortschutz nutzen, wenn sinnvoll
- Freigaben regelmäßig prüfen
- öffentliche Links vermeiden, wenn vertrauliche Daten enthalten sind

---

Umgang mit Kundendaten

Kundendaten sind besonders schützenswert.

Grundregeln:

- nur für dienstliche Zwecke nutzen
- nicht privat speichern
- nicht an Unbefugte weitergeben
- nicht in unsicheren Chats teilen
- nicht in privaten Cloudspeichern ablegen
- nur notwendige Daten verwenden
- Zugriffsrechte beachten
- Daten löschen, wenn sie nicht mehr benötigt werden und keine Aufbewahrungspflicht besteht

---

Bezug zur IT-Sicherheit

Verantwortungsvoller Umgang mit digitalen Medien hat auch mit IT-Sicherheit zu tun.

Beispiele:

- keine vertraulichen Informationen in unsicheren Kanälen
- keine Passwörter per Klartext senden
- keine unbekannten Links öffnen

- keine sensiblen Anhänge an falsche Empfänger
- Vorsicht bei Phishing
- Berechtigungen prüfen
- sichere Kommunikationswege nutzen

Bezug zur Prüfung

In der Prüfung können Situationen beschrieben werden, bei denen du richtiges oder falsches Verhalten im Umgang mit digitalen Medien erkennen sollst.

Typische Aufgaben:

- Persönlichkeitsrechte erkennen
- unzulässige Weitergabe von Informationen beurteilen
- richtige digitale Kommunikationsweise auswählen
- falsche Adressatenlisten erkennen
- Screenshot-Risiken bewerten
- Cloud-Freigaben beurteilen
- Datenschutz und Kommunikation zusammen betrachten
- Auswirkungen des eigenen Informationsverhaltens erklären

Typische Prüfungsfrage 1

Was bedeutet verantwortungsvoller Umgang mit digitalen Medien?

Antwort anzeigen

Verantwortungsvoller Umgang mit digitalen Medien bedeutet, digitale Medien bewusst, sicher, respektvoll und rechtlich korrekt zu nutzen.

Typische Prüfungsfrage 2

Warum sind Persönlichkeitsrechte bei digitaler Zusammenarbeit wichtig?

Antwort anzeigen

Persönlichkeitsrechte schützen die Privatsphäre, Würde und persönlichen Daten von Menschen. Digitale Inhalte wie Fotos, Screenshots oder personenbezogene Informationen dürfen nicht unbedacht gespeichert oder weitergegeben werden.

Typische Prüfungsfrage 3

Nenne drei Beispiele für digitale Medien im Betrieb.

Antwort anzeigen

Beispiele sind E-Mail, Chat, Ticketsystem, Videokonferenz, Cloudspeicher, Intranet, Wiki, Messenger und Projektmanagement-Tools.

Typische Prüfungsfrage 4

Warum ist ein Screenshot im Supportfall manchmal riskant?

Antwort anzeigen

Ein Screenshot kann Kundendaten, personenbezogene Daten, interne Systeme, Zugangsdaten oder vertrauliche Informationen sichtbar machen.

Typische Prüfungsfrage 5

Was sollte man vor der Weitergabe digitaler Inhalte prüfen?

Antwort anzeigen

Man sollte prüfen, ob die Weitergabe erlaubt ist, ob der Empfänger berechtigt ist, ob personenbezogene oder vertrauliche Daten enthalten sind und ob der Übertragungsweg sicher ist.

Typische Prüfungsfrage 6

Warum ist „Allen antworten“ bei E-Mails manchmal problematisch?

Antwort anzeigen

Weil dadurch Informationen an Personen gelangen können, die diese nicht benötigen oder nicht erhalten dürfen. Das kann Datenschutz- oder Vertraulichkeitsprobleme verursachen.

Typische Prüfungsfrage 7

Was ist gutes Kommunikationsverhalten in digitalen Medien?

Antwort anzeigen

Gutes Kommunikationsverhalten ist sachlich, höflich, verständlich, zielgerichtet, respektvoll, empfängerorientiert, datenschutzbewusst und sicherheitsbewusst.

Typische Prüfungsfrage 8

Was bedeutet gutes Informationsverhalten?

Antwort anzeigen

Gutes Informationsverhalten bedeutet, Informationen zu prüfen, vertrauliche Daten zu schützen, nur notwendige Daten zu speichern, Berechtigungen zu beachten und Informationen nicht ungeprüft weiterzugeben.

Typische Prüfungsfrage 9

Warum sollte man Cloud-Freigaben regelmäßig prüfen?

Antwort anzeigen

Weil Freigaben sonst zu lange bestehen bleiben, falsche Personen Zugriff haben können oder vertrauliche Daten unberechtigt erreichbar sind.

Typische Prüfungsfrage 10

Warum sollte man digitale Inhalte vor dem Teilen sorgfältig prüfen?

Antwort anzeigen

Digitale Inhalte können schnell kopiert, weitergeleitet und lange gespeichert werden. Fehlerhafte oder vertrauliche Inhalte lassen sich oft schwer zurückholen.

Merksatz

- Digitale Medien müssen bewusst, sicher und respektvoll genutzt werden
- Persönlichkeitsrechte schützen Privatsphäre, Würde und persönliche Daten

- Nicht alles, was technisch möglich ist, ist erlaubt oder sinnvoll
- Vor dem Speichern, Darstellen und Weitergeben digitaler Inhalte immer Zweck, Empfänger und Inhalt prüfen
- Screenshots können sensible Daten enthalten
- Cloud-Freigaben und Links müssen gezielt und begrenzt vergeben werden
- Gute digitale Kommunikation ist sachlich, höflich, klar und datenschutzbewusst
- Gutes Informationsverhalten bedeutet: prüfen, schützen, gezielt weitergeben

Seite 5.3 Informationstechnische Schutzziele bei der Kommunikation

Prüfungsziel

Du sollst erklären können, welche informationstechnischen Schutzziele bei digitaler Kommunikation wichtig sind und wie man sie im privaten und betrieblichen Bereich beachtet.

Für die Prüfung sind hier vor allem wichtig:

- informationstechnische Schutzziele bei der Kommunikation
- Sicherheitsbewusstsein bei der Nutzung von IT-Technik
- IT-Sicherheit im privaten und betrieblichen Bereich
- Erfahrungen in virtuellen Räumen reflektieren
- Gefahren bei Social Media kennen
- Zuständigkeitsabgrenzung bei Kommunikation und Information
- sicherer Umgang mit dienstlichen E-Mails
- kurzer, zielführender, höflicher und korrekter Informationsaustausch
- Netiquette
- Nachrichten aus Sicht der Empfänger betrachten
- sensibler Umgang mit Adressatenlisten
- mögliche juristische Konsequenzen von Äußerungen über den Arbeitgeber
- Social Engineering erkennen und Schäden vermeiden

Was sind informationstechnische Schutzziele?

Informationstechnische Schutzziele beschreiben, was bei Informationen und IT-Systemen geschützt werden soll.

Die wichtigsten Schutzziele sind:

Schutzziel	Bedeutung
Vertraulichkeit	Informationen dürfen nur berechtigte Personen sehen
Integrität	Informationen dürfen nicht unbemerkt verändert werden
Verfügbarkeit	Informationen und Systeme müssen bei Bedarf nutzbar sein
Authentizität	Absender, Nutzer oder Systeme müssen echt und überprüfbar sein
Nachvollziehbarkeit	Vorgänge sollen später nachvollzogen werden können

---

Vertraulichkeit

Vertraulichkeit bedeutet, dass Informationen nur für berechtigte Personen zugänglich sind.

Beispiele:

- Kundendaten nicht an falsche Empfänger senden
- Passwörter nicht per Klartext verschicken
- interne Dokumente nicht öffentlich teilen
- E-Mails nur an berechtigte Personen senden
- Screenshots vor Weitergabe prüfen
- Cloud-Freigaben begrenzen

Beispiel aus der IT:

Ein Screenshot aus einem Ticketsystem enthält Kundendaten.

Vor dem Versenden müssen sensible Daten geschwärzt oder entfernt werden.

Integrität

Integrität bedeutet, dass Informationen vollständig und unverändert bleiben.

Beispiele:

- Dokumente dürfen nicht unbemerkt verändert werden
- Konfigurationsdateien müssen korrekt bleiben
- Logdateien dürfen nicht manipuliert werden
- Anhänge dürfen nicht durch Schadsoftware verändert werden
- Arbeitsanweisungen müssen aktuell und richtig sein

Beispiel aus der IT:

Eine Konfigurationsdatei wird per E-Mail verschickt.

Wenn sie unterwegs verändert wird, kann ein System falsch eingerichtet werden.

Verfügbarkeit

Verfügbarkeit bedeutet, dass Informationen, Systeme und Kommunikationsmittel bei Bedarf nutzbar sind.

Beispiele:

- E-Mail-System funktioniert
- Ticketsystem ist erreichbar
- VPN-Zugang steht bereit
- interne Wiki-Seiten sind verfügbar

- Telefonie und Chat funktionieren
- wichtige Dokumente sind nicht nur lokal auf einem Gerät gespeichert

Beispiel aus der IT:

Wenn das Ticketsystem ausfällt, können Störungen schlechter bearbeitet werden.

Deshalb sind Backups, Monitoring und Notfallpläne wichtig.

Authentizität

Authentizität bedeutet, dass eine Person, Nachricht oder ein System echt ist.

Beispiele:

- Absender einer E-Mail prüfen
- verdächtige Links nicht anklicken
- Identität am Telefon prüfen
- digitale Signaturen nutzen
- Zertifikate prüfen
- keine Zugangsdaten an unbekannte Personen herausgeben

Beispiel:

Eine E-Mail sieht aus, als käme sie vom Geschäftsführer und fordert eine schnelle Überweisung.

Vor dem Handeln muss geprüft werden, ob die Nachricht wirklich echt ist.

Nachvollziehbarkeit

Nachvollziehbarkeit bedeutet, dass Handlungen später geprüft oder verstanden werden können.

Beispiele:

- Tickets sauber dokumentieren
- Änderungen an Systemen protokollieren
- Entscheidungen schriftlich festhalten
- E-Mail-Verläufe geordnet ablegen
- Berechtigungsänderungen dokumentieren
- wichtige Anweisungen nicht nur mündlich geben

Beispiel aus dem Support:

Wenn ein Ticket ohne Dokumentation geschlossen wird, kann später niemand nachvollziehen, was gemacht wurde.

Sicherheitsbewusstsein bei IT-Nutzung

Sicherheitsbewusstsein bedeutet, mögliche Gefahren zu erkennen und vorsichtig mit IT-Systemen und Informationen umzugehen.

Einfach gesagt:

Man denkt mit, bevor man klickt, sendet, speichert oder teilt.

Wichtig im Betrieb:

- keine unbekannten Anhänge öffnen
- Links prüfen
- starke Passwörter nutzen
- MFA verwenden, wenn vorgesehen
- Geräte sperren, wenn man den Arbeitsplatz verlässt
- keine vertraulichen Daten offen liegen lassen
- verdächtige Vorfälle melden
- private und dienstliche Nutzung trennen
- Sicherheitsrichtlinien beachten

IT-Sicherheit im privaten und betrieblichen Bereich

IT-Sicherheit betrifft nicht nur den Arbeitsplatz.

Auch privates Verhalten kann den Betrieb beeinflussen.

Beispiele:

- dienstliche E-Mails auf privaten Geräten
- private Cloudspeicher für Firmendaten
- schwache Passwörter
- gleiche Passwörter privat und dienstlich
- Social-Media-Beiträge über den Arbeitgeber
- Phishing über private Messenger
- unsichere WLAN-Netze

Wichtig:

Dienstliche Daten gehören nicht unkontrolliert in private Systeme.

Virtuelle Räume

Virtuelle Räume sind digitale Umgebungen, in denen Menschen zusammenarbeiten oder kommunizieren.

Beispiele:

- Videokonferenz
- Chat
- Online-Meeting
- Cloud-Dokument
- Ticketsystem
- Lernplattform
- Social-Media-Gruppe
- Forum
- Online-Projektboard

Erfahrungen in virtuellen Räumen reflektieren

Reflektieren bedeutet, das eigene Verhalten zu überdenken.

Fragen zur Reflexion:

- War meine Nachricht klar?
- War der Ton angemessen?
- Habe ich die richtigen Empfänger gewählt?
- Habe ich vertrauliche Inhalte geschützt?
- Habe ich andere ausreden lassen?
- Habe ich unnötige Informationen geteilt?
- Habe ich Missverständnisse verursacht?
- War der Kommunikationskanal passend?

Social Media und IT-Sicherheit

Social Media kann private und betriebliche Risiken verursachen.

Risiken:

- Informationen über Arbeitgeber werden öffentlich
- Angreifer sammeln Informationen über Mitarbeiter
- Phishing über soziale Netzwerke
- gefälschte Profile
- Rufschädigung
- Preisgabe interner Projekte
- Veröffentlichung vertraulicher Informationen
- unbedachte Kommentare
- Verletzung von Persönlichkeitsrechten

Beispiel: Social-Media-Risiko

Ein Mitarbeiter postet:

„Heute wieder Chaos im Serverraum. Kunde XY ist seit Stunden offline.“

Problem:

- Kundenname wird öffentlich
- interner Vorfall wird bekannt
- Imageschaden möglich
- Vertraulichkeit verletzt
- arbeitsrechtliche Folgen möglich

Zuständigkeitsabgrenzung bei Kommunikation und Information

Zuständigkeitsabgrenzung bedeutet, dass klar ist, wer welche Informationen geben darf und wer wofür verantwortlich ist.

Warum ist das wichtig?

Nicht jeder darf jede Auskunft geben.

Beispiele:

Situation	Zuständig
Presseanfrage	Geschäftsführung oder Pressestelle
Datenschutzvorfall	Datenschutzbeauftragter / zuständige Stelle
IT-Sicherheitsvorfall	IT-Sicherheitsverantwortliche
Kundenbeschwerde	zuständiger Kundenbetreuer
Vertragsfrage	Vertrieb oder Rechtsabteilung
Personalfrage	Personalabteilung
technische Störung	IT-Support oder Fachteam

Beispiel für falsche Zuständigkeitsabgrenzung

Ein Azubi antwortet einem Kunden eigenständig auf eine rechtliche Frage zum Datenschutz.

Problem:

Der Azubi ist dafür wahrscheinlich nicht zuständig.

Richtiges Verhalten:

- Anfrage aufnehmen

- keine verbindliche Aussage machen
- an zuständige Stelle weiterleiten
- Rückmeldung dokumentieren

Sicherer Umgang mit dienstlichen E-Mails

Dienstliche E-Mails müssen sorgfältig, höflich und sicher geschrieben werden.

Wichtige Regeln:

- klare Betreffzeile
- höfliche Anrede
- kurze und verständliche Formulierung
- sachlicher Ton
- richtige Empfänger auswählen
- CC und BCC bewusst nutzen
- Anhänge prüfen
- vertrauliche Inhalte schützen
- keine Passwörter im Klartext senden
- vor dem Senden nochmal prüfen
- keine unbestätigten Informationen verbreiten

Kurzer, zielführender, höflicher und korrekter Informationsaustausch

Eine gute dienstliche E-Mail ist:

Eigenschaft	Bedeutung
kurz	keine unnötigen Informationen
zielführend	Empfänger erkennt, was zu tun ist
höflich	respektvoller Ton
korrekt	sachlich richtig und sprachlich angemessen
vollständig	wichtige Informationen fehlen nicht
sicher	keine unnötigen vertraulichen Daten

Beispiel für schlechte E-Mail

```
Betreff: Problem

Hi,
geht nicht. Bitte schnell machen.
```

Gruß

Problem:

- unklarer Betreff
- keine genaue Fehlerbeschreibung
- kein System genannt
- keine Dringlichkeit begründet
- nicht zielführend

Beispiel für bessere E-Mail

Betreff: VPN-Zugang für Benutzer Müller funktioniert seit 09:30 Uhr nicht

Hallo Support-Team,

der Benutzer Max Müller kann sich seit ca. 09:30 Uhr nicht mehr per VPN verbinden.
Fehlermeldung: „Authentifizierung fehlgeschlagen“.
Ein Neustart des Clients wurde bereits versucht.

Bitte prüft den Zugang.

Viele Grüße

Warum besser?

- klarer Betreff
- konkrete Beschreibung
- Zeitpunkt genannt
- Fehlermeldung genannt
- bisherige Schritte genannt
- höflich und sachlich

Netiquette

Netiquette bedeutet höfliche und angemessene Umgangsformen in digitaler Kommunikation.

Wichtige Netiquette-Regeln:

- höflich bleiben
- sachlich schreiben
- keine Beleidigungen
- keine komplett großgeschriebenen Nachrichten
- Ironie vorsichtig einsetzen

- andere ausreden lassen
- keine unnötigen Nachrichtenfluten
- passende Kanäle nutzen
- keine vertraulichen Inhalte in öffentliche Kanäle
- vor dem Senden nachdenken

Nachrichten aus Sicht der Empfänger betrachten

Bevor eine Nachricht gesendet wird, sollte man überlegen, wie sie beim Empfänger ankommt.

Fragen:

- Ist die Nachricht verständlich?
- Ist der Ton respektvoll?
- Weiß der Empfänger, was zu tun ist?
- Fehlen wichtige Informationen?
- Sind zu viele Informationen enthalten?
- Könnte die Nachricht falsch verstanden werden?
- Darf der Empfänger diese Informationen sehen?

Sensibler Umgang mit Adressatenlisten

Adressatenlisten müssen sorgfältig verwendet werden.

Begriffe:

Feld	Bedeutung
An	direkte Empfänger
CC	Personen erhalten die Nachricht zur Kenntnis
BCC	Empfänger sind für andere nicht sichtbar

Risiken bei Adressatenlisten

Fehler	Risiko
falscher Empfänger	vertrauliche Informationen gelangen an falsche Person
zu viele Personen in CC	unnötige Informationsweitergabe
offene Verteilerliste	E-Mail-Adressen werden sichtbar
kein BCC bei großen Gruppen	Datenschutzproblem möglich
„Allen antworten“ unüberlegt	Informationen werden unnötig verbreitet

---

Beispiel: Adressatenfehler

Eine E-Mail mit Kundendaten wird versehentlich an einen externen Empfänger mit ähnlichem Namen gesendet.

Mögliche Folgen:

- Datenschutzvorfall
- Meldepflicht möglich
- Vertrauensverlust
- interne Nacharbeit
- Schulungsbedarf

Richtiges Verhalten:

- Empfänger vor dem Senden prüfen
- Autovervollständigung kontrollieren
- bei sensiblen Daten besondere Vorsicht
- Fehler sofort melden

Äußerungen über den Arbeitgeber in sozialen Netzwerken

Äußerungen über den Arbeitgeber können Konsequenzen haben.

Problematisch sind zum Beispiel:

- Beleidigungen
- Veröffentlichung interner Informationen
- Kundendaten
- Geschäftsgeheimnisse
- Fotos aus gesicherten Bereichen
- falsche Behauptungen
- Rufschädigung
- vertrauliche Projektinformationen

Wichtig:

Auch private Beiträge können arbeitsrechtliche oder juristische Folgen haben, wenn sie den Arbeitgeber, Kunden oder Kollegen betreffen.

Beispiel für problematischen Beitrag

```
Unser Chef hat keine Ahnung. Außerdem ist Kunde XY wegen unserer schlechten IT gerade komplett lahmgelegt.
```

Problem:

- beleidigende Aussage
- Kundendaten oder Kundenbezug
- interne Störung öffentlich gemacht
- Rufschädigung
- mögliche arbeitsrechtliche Folgen

Social Engineering

Social Engineering bedeutet, dass Angreifer Menschen manipulieren, um an Informationen, Zugänge oder Handlungen zu kommen.

Einfach gesagt:

Nicht die Technik wird zuerst angegriffen, sondern der Mensch.

Typische Social-Engineering-Methoden

Methode	Erklärung
Phishing	gefälschte E-Mail oder Website
Spear-Phishing	gezieltes Phishing gegen bestimmte Personen
Vishing	Betrug per Telefon
Smishing	Betrug per SMS oder Messenger
Pretexting	Angreifer gibt falsche Identität oder Geschichte vor
Tailgating	Angreifer folgt unberechtigt durch eine Tür
CEO-Fraud	angebliche Anweisung der Geschäftsführung
USB-Drop	präparierter USB-Stick wird absichtlich platziert

Beispiel: Social Engineering per Telefon

Eine Person ruft im Unternehmen an und sagt:

„Ich bin vom IT-Support. Wir müssen Ihr Konto prüfen. Bitte nennen Sie mir Ihr Passwort.“

Richtiges Verhalten:

- Passwort niemals nennen
- Identität prüfen
- Gespräch beenden, wenn verdächtig
- Vorfall melden

- zuständige IT-Sicherheitsstelle informieren

Warnzeichen für Social Engineering

- ungewöhnlicher Zeitdruck
- Drohungen oder Druck
- Bitte um Passwort oder Zugangscode
- ungewöhnliche Zahlungsaufforderung
- unbekannter Absender
- gefälschte E-Mail-Adresse
- unerwarteter Anhang
- verdächtiger Link
- Bitte um Umgehung von Regeln
- Geheimhaltung wird verlangt

Schäden durch Social Engineering vermeiden

Wichtige Maßnahmen:

- Sicherheitsbewusstsein entwickeln
- Passwörter nie weitergeben
- Identität von Anfragenden prüfen
- verdächtige E-Mails melden
- Links prüfen
- Anhänge nur bei vertrauenswürdiger Quelle öffnen
- keine fremden USB-Sticks verwenden
- Besucherregeln beachten
- keine Türen für Unberechtigte öffnen
- klare Meldewege nutzen
- Schulungen ernst nehmen

Bezug zur Prüfung

In der Prüfung können Situationen beschrieben werden, bei denen du entscheiden sollst, welches Verhalten sicher und korrekt ist.

Typische Aufgaben:

- Schutzziele zuordnen
- Vertraulichkeit bei E-Mails erkennen
- Fehler bei Adressatenlisten bewerten
- Social Engineering erkennen
- sichere E-Mail-Kommunikation auswählen
- Netiquette-Regeln anwenden

- Social-Media-Äußerungen beurteilen
- Zuständigkeiten richtig einordnen

Typische Prüfungsfrage 1

Nenne drei informationstechnische Schutzziele.

Antwort anzeigen

Drei wichtige Schutzziele sind Vertraulichkeit, Integrität und Verfügbarkeit.

Typische Prüfungsfrage 2

Was bedeutet Vertraulichkeit?

Antwort anzeigen

Vertraulichkeit bedeutet, dass Informationen nur für berechtigte Personen zugänglich sind.

Typische Prüfungsfrage 3

Was bedeutet Integrität?

Antwort anzeigen

Integrität bedeutet, dass Informationen vollständig und unverändert bleiben und nicht unbemerkt manipuliert werden.

Typische Prüfungsfrage 4

Was bedeutet Verfügbarkeit?

Antwort anzeigen

Verfügbarkeit bedeutet, dass Informationen, Systeme und Dienste bei Bedarf nutzbar sind.

Typische Prüfungsfrage 5

Warum ist Authentizität bei Kommunikation wichtig?

Antwort anzeigen

Weil geprüft werden muss, ob Absender, Nachricht oder System echt sind. Dadurch können gefälschte Nachrichten und Betrugsversuche erkannt werden.

Typische Prüfungsfrage 6

Was bedeutet Netiquette?

Antwort anzeigen

Netiquette bedeutet höfliche und angemessene Umgangsformen in digitaler Kommunikation.

Typische Prüfungsfrage 7

Warum muss man Adressatenlisten sorgfältig prüfen?

Antwort anzeigen

Weil vertrauliche oder personenbezogene Informationen sonst an falsche oder zu viele Personen gelangen können.

Typische Prüfungsfrage 8

Warum können Äußerungen über den Arbeitgeber in sozialen Netzwerken problematisch sein?

Antwort anzeigen

Weil sie interne Informationen, Kundendaten, Geschäftsgeheimnisse oder beleidigende Aussagen enthalten können. Das kann arbeitsrechtliche oder juristische Folgen haben.

Typische Prüfungsfrage 9

Was ist Social Engineering?

Antwort anzeigen

Social Engineering ist eine Angriffsmethode, bei der Menschen manipuliert werden, um Informationen, Zugangsdaten oder bestimmte Handlungen zu erhalten.

Typische Prüfungsfrage 10

Nenne drei Warnzeichen für Social Engineering.

Antwort anzeigen

Warnzeichen sind zum Beispiel ungewöhnlicher Zeitdruck, Bitte um Passwörter, verdächtige Links, unbekannte Absender, Drohungen oder die Aufforderung, Regeln zu umgehen.

Merksatz

- Vertraulichkeit = nur Berechtigte dürfen Informationen sehen
- Integrität = Informationen bleiben korrekt und unverändert
- Verfügbarkeit = Systeme und Informationen sind nutzbar
- Authentizität = Echtheit von Absendern, Nutzern und Systemen
- Netiquette = höfliche digitale Umgangsformen
- E-Mails müssen kurz, zielführend, höflich, korrekt und sicher sein
- Adressatenlisten immer sorgfältig prüfen
- Social Media kann arbeitsrechtliche und juristische Folgen haben
- Social Engineering greift den Menschen an, nicht nur die Technik
- Passwörter niemals weitergeben

Seite 5.4 Compliance, Diversity und ethische Aspekte bei IT-Lösungen

Prüfungsziel

Du sollst erklären können, warum IT-Lösungen nicht nur technisch funktionieren müssen, sondern auch rechtlich, ethisch und sozial verantwortungsvoll gestaltet und genutzt werden sollen.

Für die Prüfung sind hier vor allem wichtig:

- Compliance
- betriebliche Regeln
- ethische Aspekte bei IT-Lösungen
- Diversity
- Gender-Neutralität
- Würde und Integrität von Menschen
- verantwortungsbewusster Umgang mit Technik
- Auswirkungen von IT-Systemen auf Menschen
- faire und diskriminierungsfreie digitale Prozesse

Was bedeutet Compliance?

Compliance bedeutet, dass sich ein Unternehmen und seine Beschäftigten an Gesetze, Vorschriften, interne Regeln und ethische Grundsätze halten.

Einfach gesagt:

Compliance bedeutet: Regeln einhalten.

Dazu gehören zum Beispiel:

- Gesetze
- Datenschutzvorgaben
- IT-Sicherheitsrichtlinien
- Arbeitsanweisungen
- Betriebsvereinbarungen
- Verhaltenskodex
- Unternehmenswerte
- Vorgaben zum Umgang mit Kunden und Daten
- Regeln zur Nutzung von IT-Systemen

Warum ist Compliance wichtig?

Compliance schützt das Unternehmen, die Beschäftigten, Kunden und Geschäftspartner.

Vorteile:

- rechtliche Sicherheit
- weniger Datenschutzverstöße
- weniger Sicherheitsvorfälle
- Schutz vor Bußgeldern
- Schutz des Unternehmensimages
- klare Regeln für Mitarbeiter
- mehr Vertrauen bei Kunden
- weniger Missbrauch von IT-Systemen

Beispiele für Compliance im IT-Bereich

Situation	Compliance-Anforderung
Umgang mit Kundendaten	Datenschutzregeln einhalten
Nutzung von Software	nur lizenzierte Software verwenden
Passwörter	Sicherheitsrichtlinien beachten
Zugriff auf Systeme	nur berechtigte Zugriffe nutzen
E-Mail-Kommunikation	vertrauliche Daten schützen
Dokumentation	Änderungen nachvollziehbar dokumentieren
Social Media	keine Geschäftsgeheimnisse veröffentlichen
Beschaffung	Vorgaben für Einkauf und Nachhaltigkeit beachten

Beispiel: Softwarelizenz

Ein Mitarbeiter installiert eine kostenpflichtige Software ohne gültige Lizenz auf einem Firmenrechner.

Problem:

- Verstoß gegen Lizenzrecht
- rechtliches Risiko für das Unternehmen
- mögliche Kosten oder Vertragsstrafen
- Verstoß gegen interne IT-Regeln

Richtiges Verhalten:

- Softwarebedarf melden
- Lizenz prüfen lassen
- Freigabe durch zuständige Stelle abwarten

- nur erlaubte Software installieren

Beispiel: Zugriff auf Kundendaten

Ein Mitarbeiter schaut Kundendaten an, obwohl er sie für seine Aufgabe nicht benötigt.

Problem:

- Verstoß gegen Datenschutz
- Verstoß gegen Berechtigungskonzept
- möglicher Vertrauensverlust
- rechtliche Folgen möglich

Richtiges Verhalten:

Nur Daten einsehen, die für die eigene Aufgabe erforderlich sind.

Betriebliche Regeln

Betriebliche Regeln legen fest, wie Beschäftigte im Unternehmen handeln sollen.

Beispiele:

- IT-Nutzungsrichtlinie
- Passwortregel
- Datenschutzrichtlinie
- E-Mail-Richtlinie
- Clean-Desk-Regel
- Homeoffice-Regel
- Regelung zur privaten Internetnutzung
- Social-Media-Richtlinie
- Meldeweg bei Sicherheitsvorfällen
- Richtlinie zur Nutzung von KI-Werkzeugen

Warum sind betriebliche Regeln wichtig?

Sie sorgen dafür, dass alle wissen, was erlaubt ist und was nicht.

Beispiele:

Regel	Zweck
Passwortregel	Schutz von Benutzerkonten
Datenschutzrichtlinie	Schutz personenbezogener Daten

Regel	Zweck
IT-Nutzungsrichtlinie	sichere und erlaubte Nutzung von IT
Social-Media-Richtlinie	Schutz vor Rufschädigung und Datenabfluss
Meldeweg bei Vorfällen	schnelle Reaktion bei Sicherheitsproblemen
Homeoffice-Regel	Sicherheit und Datenschutz außerhalb des Betriebs

---

Ethische Aspekte bei IT-Lösungen

Ethik bedeutet, sich mit richtigem und verantwortungsvollem Handeln zu beschäftigen.

Bei IT-Lösungen geht es nicht nur darum, ob etwas technisch möglich ist.

Es geht auch darum:

- Ist es fair?
- Ist es erlaubt?
- Ist es transparent?
- Schadet es Menschen?
- Werden Menschen benachteiligt?
- Werden Daten verantwortungsvoll genutzt?
- Können Betroffene die Entscheidung nachvollziehen?
- Wird die Würde von Menschen respektiert?

Technisch möglich heißt nicht automatisch richtig

In der IT kann man viele Dinge technisch umsetzen.

Aber nicht alles, was technisch möglich ist, ist auch sinnvoll, erlaubt oder ethisch vertretbar.

Beispiele:

Technisch möglich	Problem
alle Mitarbeiter dauerhaft überwachen	Eingriff in Persönlichkeitsrechte
Kundendaten unbegrenzt speichern	Datenschutzproblem
Bewerber automatisch aussortieren	Diskriminierungsrisiko
private Chatverläufe auswerten	Verletzung der Privatsphäre
Standortdaten dauerhaft speichern	Überwachung und Datenschutzproblem
KI ohne Kontrolle entscheiden lassen	fehlende Nachvollziehbarkeit

---

Beispiel: Überwachung am Arbeitsplatz

Ein Unternehmen möchte eine Software einsetzen, die jede Tastatureingabe, Mausbewegung und Bildschirmaktivität der Mitarbeiter dauerhaft protokolliert.

Technisch möglich:

Ja.

Problematisch wegen:

- Persönlichkeitsrechten
- Datenschutz
- Vertrauensverlust
- möglicher Mitbestimmung des Betriebsrats
- Verhältnismäßigkeit
- psychischer Belastung

Prüfungsnah:

Eine technische Lösung muss verhältnismäßig, rechtlich zulässig und ethisch vertretbar sein.

Verhältnismäßigkeit

Verhältnismäßigkeit bedeutet, dass eine Maßnahme geeignet, erforderlich und angemessen sein muss.

Einfach gesagt:

Eine Maßnahme darf nicht stärker in Rechte eingreifen als nötig.

Beispiel:

Ziel: IT-Sicherheit verbessern.

Möglichkeit A:

- alle Mitarbeiter dauerhaft per Bildschirmaufnahme überwachen

Möglichkeit B:

- Protokollierung sicherheitsrelevanter Systemereignisse
- Rollen- und Rechtekonzept
- Schulungen
- MFA
- Sicherheitsmonitoring

Bewertung:

Möglichkeit B ist meistens verhältnismäßiger, weil sie weniger stark in Persönlichkeitsrechte eingreift.

Transparenz

Transparenz bedeutet, dass Betroffene verstehen können, was mit ihren Daten passiert und warum.

Beispiele:

- Mitarbeiter wissen, welche Daten protokolliert werden
- Kunden erhalten verständliche Datenschutzhinweise
- Berechtigungen sind nachvollziehbar
- automatisierte Entscheidungen werden erklärt
- Änderungen an Systemen werden dokumentiert

Verantwortung bei IT-Lösungen

Wer IT-Systeme plant, einführt oder betreut, trägt Verantwortung.

Verantwortung besteht gegenüber:

- Benutzern
- Kunden
- Kollegen
- Arbeitgeber
- Gesellschaft
- Datenschutz
- IT-Sicherheit
- Umwelt
- rechtlichen Vorgaben

Beispiel:

Ein Fachinformatiker richtet Benutzerrechte ein.

Wenn Rechte zu weit vergeben werden, können vertrauliche Daten unberechtigt eingesehen werden.

Deshalb müssen Rechte sorgfältig und nach dem Prinzip „so viel wie nötig, so wenig wie möglich“ vergeben werden.

Diversity

Diversity bedeutet Vielfalt.

Im Betrieb meint Diversity, dass Menschen unterschiedliche Eigenschaften, Erfahrungen und Hintergründe haben.

Beispiele für Vielfalt:

- Alter
- Geschlecht
- Sprache
- Herkunft
- Kultur
- Religion
- Behinderung
- Bildungsweg
- Berufserfahrung
- Lebenssituation
- Arbeitsweise

Warum ist Diversity wichtig?

Vielfalt kann Teams stärker machen.

Vorteile:

- unterschiedliche Perspektiven
- bessere Problemlösung
- mehr Kreativität
- bessere Nutzerorientierung
- fairere Entscheidungen
- weniger einseitige Sichtweisen
- bessere Zusammenarbeit mit unterschiedlichen Kunden

Wichtig:

Diversity bedeutet nicht nur, Unterschiede zu erkennen.
Es bedeutet auch, fair und respektvoll damit umzugehen.

Diversity bei IT-Lösungen

IT-Lösungen sollten möglichst viele Nutzergruppen berücksichtigen.

Beispiele:

- einfache und verständliche Sprache
- barrierearme Bedienung
- gute Kontraste

- Tastaturbedienung
- Unterstützung für Screenreader
- verständliche Fehlermeldungen
- mehrsprachige Informationen, wenn nötig
- keine diskriminierenden Auswahlkriterien
- Schulungen für unterschiedliche Vorkenntnisse

Beispiel: Barrierearme IT-Lösung

Ein internes Ticketsystem wird eingeführt.

Dabei sollte geprüft werden:

- Ist die Schrift gut lesbar?
- Gibt es ausreichende Kontraste?
- Kann man das System mit Tastatur bedienen?
- Sind Fehlermeldungen verständlich?
- Können auch neue Mitarbeiter das System nutzen?
- Werden unterschiedliche Sprachkenntnisse berücksichtigt?
- Gibt es Schulungen?

Gender-Neutralität

Gender-Neutralität bedeutet, Menschen unabhängig vom Geschlecht fair und respektvoll anzusprechen und nicht unnötig auszuschließen.

Beispiele für genderneutrale Formulierungen:

Nicht optimal	Besser
Mitarbeiter müssen ihr Passwort ändern	Beschäftigte müssen ihr Passwort ändern
Jeder Benutzer bekommt eine Rolle	Jede Person erhält eine Rolle
Ansprechpartner	Ansprechperson
Teilnehmerliste	Teilnehmendenliste
Administratorenrechte	Administrationsrechte

Wichtig:

In Prüfungen geht es meist nicht um Sprachpolitik, sondern um respektvolle, faire und inklusive Kommunikation.

Gender-Neutralität in IT-Systemen

Auch IT-Systeme können genderneutral gestaltet werden.

Beispiele:

- Formulare bieten passende Auswahlmöglichkeiten
- Pflichtfelder sind sinnvoll begrenzt
- Anreden sind respektvoll
- Texte schließen niemanden unnötig aus
- Benutzerrollen sind sachlich benannt
- Systeme erzwingen keine unnötigen Angaben

Beispiel:

Ein Formular fragt nach dem Geschlecht, obwohl es für den Zweck nicht notwendig ist.

Problem:

- unnötige Datenerhebung
- mögliche Diskriminierung
- Datenschutzprinzip der Datenminimierung wird berührt

Würde des Menschen

Die Würde des Menschen bedeutet, dass jeder Mensch respektvoll behandelt werden muss.

Im Betrieb heißt das:

- keine Beleidigung
- keine Bloßstellung
- keine Diskriminierung
- kein Mobbing
- keine entwürdigende Überwachung
- respektvoller Umgang mit Fehlern
- Schutz der Privatsphäre
- faire Behandlung

Integrität von Menschen

Integrität bedeutet Unversehrtheit, Selbstbestimmung und Achtung der Persönlichkeit.

Im IT-Kontext bedeutet das:

- Menschen nicht manipulieren
- persönliche Daten schützen
- keine unnötige Überwachung
- keine diskriminierenden Systeme

- transparente Entscheidungen
- faire Behandlung
- Schutz vor digitaler Bloßstellung

Beispiel: Würde und Integrität

Ein Team veröffentlicht im internen Chat Screenshots von Fehlern eines Kollegen und macht sich darüber lustig.

Problem:

- respektlos
- mögliche Bloßstellung
- verletzt Würde und Integrität
- schlechtes Teamklima
- kann arbeitsrechtliche Folgen haben

Richtiges Verhalten:

- Fehler sachlich ansprechen
- Unterstützung anbieten
- keine öffentliche Bloßstellung
- aus Fehlern lernen

Diskriminierung durch IT-Systeme

IT-Systeme können Menschen benachteiligen, wenn sie falsch gestaltet oder genutzt werden.

Beispiele:

- Bewerbersystem sortiert bestimmte Gruppen systematisch aus
- Software ist für Menschen mit Sehbehinderung kaum nutzbar
- Formulare lassen bestimmte Namen oder Zeichen nicht zu
- Algorithmen treffen nicht nachvollziehbare Entscheidungen
- automatische Bewertungen beruhen auf schlechten Daten
- Übersetzungen oder Texte enthalten Vorurteile

Warum können Daten problematisch sein?

IT-Systeme arbeiten oft mit Daten.

Wenn Daten fehlerhaft, unvollständig oder einseitig sind, können auch die Ergebnisse unfair sein.

Beispiel:

Ein System bewertet Bewerbungen anhand alter Daten.

Wenn früher bestimmte Gruppen seltener eingestellt wurden, kann das System diese Benachteiligung übernehmen.

Prüfungsnah:

Digitale Systeme müssen kritisch geprüft werden, besonders wenn sie Menschen bewerten oder Entscheidungen vorbereiten.

KI und ethische Verantwortung

Auch KI-Systeme müssen verantwortungsvoll genutzt werden.

Wichtige Fragen:

- Welche Daten werden genutzt?
- Sind personenbezogene Daten enthalten?
- Ist die Entscheidung nachvollziehbar?
- Gibt es menschliche Kontrolle?
- Können Fehler erkannt werden?
- Werden Menschen diskriminiert?
- Werden vertrauliche Informationen eingegeben?
- Ist die Nutzung im Betrieb erlaubt?

Beispiel: KI im Betrieb

Ein Mitarbeiter gibt vertrauliche Kundendaten in ein öffentliches KI-Tool ein, um eine E-Mail formulieren zu lassen.

Problem:

- Datenschutzrisiko
- Vertraulichkeitsverstoß
- mögliche Weitergabe sensibler Daten
- Verstoß gegen interne Regeln

Richtiges Verhalten:

- interne Regeln zur KI-Nutzung prüfen
- keine vertraulichen Daten eingeben
- Daten anonymisieren, wenn erlaubt und sinnvoll
- Ergebnisse fachlich prüfen

Ethische Entscheidung im IT-Alltag

Wenn du unsicher bist, kann diese Prüfliste helfen:

```
Ist es erlaubt?
→ Ist es notwendig?
→ Ist es fair?
→ Ist es transparent?
→ Werden Daten geschützt?
→ Werden Menschen respektiert?
→ Gibt es eine mildere Lösung?
→ Kann ich die Entscheidung begründen?
```

Bezug zur Prüfung

In der Prüfung können Situationen beschrieben werden, bei denen du beurteilen sollst, ob Verhalten oder IT-Lösungen verantwortungsvoll sind.

Typische Aufgaben:

- Compliance-Verstöße erkennen
- ethisch problematische IT-Nutzung beurteilen
- Datenschutz und Persönlichkeitsrechte beachten
- Diskriminierungsrisiken erkennen
- Gender-neutrale oder respektvolle Kommunikation auswählen
- Diversity bei IT-Lösungen berücksichtigen
- Rechts- und Regelverstöße einordnen
- angemessene Maßnahmen vorschlagen

Typische Prüfungsfrage 1

Was bedeutet Compliance?

Antwort anzeigen

Compliance bedeutet, dass sich Unternehmen und Beschäftigte an Gesetze, Vorschriften, interne Regeln und ethische Grundsätze halten.

Typische Prüfungsfrage 2

Nenne drei Beispiele für Compliance im IT-Bereich.

Antwort anzeigen

Beispiele sind Datenschutzregeln einhalten, nur lizenzierte Software verwenden, Passwortrichtlinien beachten, Zugriffsrechte nicht missbrauchen und Sicherheitsvorfälle melden.

Typische Prüfungsfrage 3

Warum ist nicht alles, was technisch möglich ist, auch automatisch erlaubt oder sinnvoll?

Antwort anzeigen

Weil technische Möglichkeiten rechtliche, ethische oder soziale Probleme verursachen können, zum Beispiel Datenschutzverstöße, Überwachung, Diskriminierung oder Verletzung von Persönlichkeitsrechten.

Typische Prüfungsfrage 4

Was bedeutet Verhältnismäßigkeit?

Antwort anzeigen

Verhältnismäßigkeit bedeutet, dass eine Maßnahme geeignet, erforderlich und angemessen sein muss. Sie darf nicht stärker in Rechte eingreifen als nötig.

Typische Prüfungsfrage 5

Was bedeutet Diversity?

Antwort anzeigen

Diversity bedeutet Vielfalt. Im Betrieb meint das unterschiedliche Eigenschaften, Erfahrungen und Hintergründe von Menschen, zum Beispiel Alter, Geschlecht, Herkunft, Sprache oder Behinderung.

Typische Prüfungsfrage 6

Warum ist Diversity bei IT-Lösungen wichtig?

Antwort anzeigen

Weil IT-Lösungen von unterschiedlichen Menschen genutzt werden. Sie sollten möglichst fair, verständlich, barrierearm und diskriminierungsfrei gestaltet sein.

Typische Prüfungsfrage 7

Was bedeutet Gender-Neutralität im betrieblichen Kontext?

Antwort anzeigen

Gender-Neutralität bedeutet, Menschen unabhängig vom Geschlecht fair und respektvoll anzusprechen und nicht unnötig auszuschließen.

Typische Prüfungsfrage 8

Nenne ein Beispiel für eine genderneutrale Formulierung.

Antwort anzeigen

Zum Beispiel „Beschäftigte“ statt „Mitarbeiter“ oder „Ansprechperson“ statt „Ansprechpartner“.

Typische Prüfungsfrage 9

Warum kann eine dauerhafte Mitarbeiterüberwachung ethisch problematisch sein?

Antwort anzeigen

Sie kann Persönlichkeitsrechte verletzen, Vertrauen zerstören, psychischen Druck erzeugen und unverhältnismäßig sein.

Typische Prüfungsfrage 10

Warum können IT-Systeme diskriminieren?

Antwort anzeigen

IT-Systeme können diskriminieren, wenn sie mit einseitigen oder fehlerhaften Daten arbeiten, bestimmte Gruppen ausschließen oder Entscheidungen nicht fair und nachvollziehbar treffen.

Typische Prüfungsfrage 11

Was muss man bei der Nutzung von KI-Werkzeugen im Betrieb beachten?

Antwort anzeigen

Man muss Datenschutz, Vertraulichkeit, interne Regeln, Nachvollziehbarkeit, mögliche Fehler und Diskriminierungsrisiken beachten. Vertrauliche Daten dürfen nicht unbedacht eingegeben werden.

Typische Prüfungsfrage 12

Was bedeutet Würde und Integrität von Menschen im digitalen Arbeitsumfeld?

Antwort anzeigen

Menschen müssen respektvoll behandelt werden. Sie dürfen nicht bloßgestellt, diskriminiert, manipuliert oder unnötig überwacht werden. Ihre Privatsphäre und Persönlichkeit müssen geschützt werden.

Merksatz

- Compliance = Regeln einhalten
- IT-Lösungen müssen nicht nur technisch, sondern auch rechtlich und ethisch passen
- Technisch möglich heißt nicht automatisch erlaubt oder richtig
- Verhältnismäßigkeit bedeutet: nicht stärker eingreifen als nötig
- Diversity = Vielfalt respektieren und berücksichtigen
- Gender-Neutralität = fair und respektvoll formulieren
- Würde und Integrität von Menschen müssen auch digital geschützt werden
- IT-Systeme können diskriminieren, wenn sie schlecht gestaltet oder mit einseitigen Daten betrieben werden
- KI-Nutzung braucht Datenschutz, Kontrolle und Verantwortung

Kompakte Wiederholung und Prüfungsfragen zu Kapitel 5

Hinweis

Diese Seite ist kein eigener Fragenkomplex im IHK-Prüfungskatalog.

Sie dient nur zum Wiederholen, Üben und Festigen der Inhalte aus Kapitel 5.

Kapitel 5 behandelt den Bereich:

Vernetztes Zusammenarbeiten unter Nutzung digitaler Medien

Kompakte Wiederholung

---

1. Wertschätzende Zusammenarbeit

Wertschätzende Zusammenarbeit bedeutet, respektvoll, fair und verantwortungsbewusst miteinander zu arbeiten.

Wichtig sind:

- respektvoller Umgang
- sachliche Kommunikation
- Zuhören
- Anerkennung der Beiträge anderer
- gemeinsame Verantwortung
- integres Verhalten
- Unternehmenswerte beachten
- betriebliche Ethikregeln beachten
- Vielfalt respektieren

Merksatz

Wertschätzende Zusammenarbeit bedeutet: fachlich zusammenarbeiten und menschlich respektvoll bleiben.

---

2. Interdisziplinarität

Interdisziplinarität bedeutet, dass Menschen aus verschiedenen Fachbereichen gemeinsam an einer Aufgabe arbeiten.

Beispiel IT-Projekt

Fachbereich	Beitrag
IT	technische Umsetzung
Datenschutz	Schutz personenbezogener Daten
Einkauf	Beschaffung
Betriebsrat	Mitbestimmung
Fachabteilung	praktische Anforderungen
Geschäftsführung	Entscheidung und Verantwortung

Merksatz

Interdisziplinarität = verschiedene Fachbereiche arbeiten gemeinsam.

---

3. Interkulturalität

Interkulturalität bedeutet, dass Menschen mit unterschiedlichen kulturellen Hintergründen zusammenarbeiten.

Wichtig sind:

- Offenheit
- Respekt
- keine Vorurteile
- klare Kommunikation
- Rücksicht auf unterschiedliche Erfahrungen
- sachlicher Umgang mit Missverständnissen

Merksatz

Interkulturalität bedeutet nicht Schubladendenken, sondern respektvoller Umgang mit Unterschieden.

---

4. Verantwortungsbewusster Umgang mit digitalen Medien

Digitale Medien müssen bewusst, sicher, respektvoll und rechtlich korrekt genutzt werden.

Beispiele für digitale Medien

- E-Mail
- Chat
- Ticketsystem
- Videokonferenz

- Cloudspeicher
- Wiki
- Intranet
- Social Media
- Projektmanagement-Tools
- Screenshots
- digitale Dokumente

Wichtig vor dem Teilen digitaler Inhalte

- Darf ich diese Information weitergeben?
- Ist der Empfänger berechtigt?
- Sind personenbezogene Daten enthalten?
- Ist die Information vertraulich?
- Ist der Kommunikationsweg sicher?
- Könnte jemand dadurch geschädigt werden?

Merksatz

Nicht alles, was technisch möglich ist, ist auch erlaubt oder sinnvoll.

---

5. Persönlichkeitsrechte

Persönlichkeitsrechte schützen Würde, Privatsphäre und persönliche Daten von Menschen.

Beispiele für geschützte Informationen

- Name
- Adresse
- E-Mail-Adresse
- Telefonnummer
- Foto
- Video
- Gesundheitsdaten
- Leistungsdaten
- private Nachrichten
- Standortdaten

Problematische Beispiele

Situation	Problem
Foto eines Kollegen ohne Zustimmung veröffentlichen	Recht am eigenen Bild
Screenshot mit Kundendaten im Chat teilen	Datenschutzrisiko
private Information über Kollegen weiterleiten	Verletzung der Privatsphäre

Situation	Problem
Videokonferenz ungefragt aufzeichnen	Persönlichkeitsrechte betroffen

Merksatz

Andere Personen dürfen digital nicht bloßgestellt, überwacht oder ohne Grund öffentlich gemacht werden.

---

6. Informationstechnische Schutzziele

Wichtige Schutzziele bei Kommunikation und IT-Nutzung sind:

Schutzziel	Bedeutung
Vertraulichkeit	nur Berechtigte dürfen Informationen sehen
Integrität	Informationen bleiben korrekt und unverändert
Verfügbarkeit	Systeme und Informationen sind nutzbar
Authentizität	Absender, Nutzer oder System sind echt
Nachvollziehbarkeit	Vorgänge können später geprüft werden

Merksatz

Vertraulichkeit, Integrität und Verfügbarkeit sind die drei klassischen Grundschutzziele.

---

7. Sichere dienstliche E-Mail-Kommunikation

Dienstliche E-Mails müssen sorgfältig geschrieben und versendet werden.

Wichtig sind:

- klare Betreffzeile
- höfliche Anrede
- sachlicher Ton
- richtige Empfänger
- CC und BCC bewusst nutzen
- Anhänge prüfen
- keine Passwörter im Klartext senden
- vertrauliche Inhalte schützen
- vor dem Senden nochmal prüfen

Merksatz

Eine gute dienstliche E-Mail ist kurz, zielführend, höflich, korrekt und sicher.

---

8. Netiquette

Netiquette bedeutet höfliche und angemessene Umgangsformen in digitaler Kommunikation.

Regeln

- höflich bleiben
- sachlich schreiben
- keine Beleidigungen
- nicht komplett in Großbuchstaben schreiben
- Ironie vorsichtig einsetzen
- passende Kanäle nutzen
- keine vertraulichen Inhalte in öffentliche Kanäle
- vor dem Senden nachdenken

Merksatz

Netiquette = gutes Benehmen im digitalen Raum.

---

9. Adressatenlisten

Adressatenlisten müssen sorgfältig geprüft werden.

Feld	Bedeutung
An	direkte Empfänger
CC	Personen erhalten die Nachricht zur Kenntnis
BCC	Empfänger sind für andere nicht sichtbar

Typische Fehler

- falscher Empfänger
- zu viele Personen in CC
- offene Verteilerliste
- „Allen antworten“ ohne Prüfung
- Autovervollständigung falsch übernommen

Merksatz

Vor dem Senden prüfen: Inhalt, Empfänger, Anhang.

---

10. Social Media

Äußerungen über Arbeitgeber, Kunden oder Kollegen in sozialen Netzwerken können problematisch sein.

Problematisch sind:

- Beleidigungen
- interne Informationen
- Kundendaten
- Geschäftsgeheimnisse
- Fotos aus geschützten Bereichen
- falsche Behauptungen
- Rufschädigung

Merksatz

Auch private Social-Media-Beiträge können berufliche Folgen haben.

---

11. Social Engineering

Social Engineering bedeutet, dass Angreifer Menschen manipulieren, um an Informationen, Zugangsdaten oder Handlungen zu kommen.

Typische Methoden

Methode	Bedeutung
Phishing	gefälschte E-Mail oder Website
Spear-Phishing	gezieltes Phishing gegen bestimmte Personen
Vishing	Betrug per Telefon
Smishing	Betrug per SMS oder Messenger
CEO-Fraud	angebliche Anweisung der Geschäftsführung
Tailgating	unberechtigtes Folgen durch eine Tür
USB-Drop	präparierter USB-Stick wird platziert

Merksatz

Social Engineering greift zuerst den Menschen an, nicht die Technik.

---

12. Compliance

Compliance bedeutet, Gesetze, Vorschriften, interne Regeln und ethische Grundsätze einzuhalten.

Beispiele im IT-Bereich

- Datenschutzregeln einhalten
- nur lizenzierte Software nutzen

- Passwortrichtlinien beachten
- Zugriffsrechte nicht missbrauchen
- Sicherheitsvorfälle melden
- keine vertraulichen Daten unberechtigt weitergeben
- interne IT-Richtlinien beachten

Merksatz

Compliance = Regeln einhalten.

---

13. Ethische Aspekte bei IT-Lösungen

IT-Lösungen müssen nicht nur technisch funktionieren.

Sie müssen auch rechtlich, sozial und ethisch vertretbar sein.

Wichtige Fragen

- Ist die Lösung erlaubt?
- Ist sie notwendig?
- Ist sie fair?
- Ist sie transparent?
- Werden Daten geschützt?
- Werden Menschen respektiert?
- Gibt es eine mildere Lösung?
- Kann die Entscheidung begründet werden?

Merksatz

Technisch möglich heißt nicht automatisch erlaubt oder richtig.

---

14. Diversity und Gender-Neutralität

Diversity bedeutet Vielfalt.

Menschen unterscheiden sich zum Beispiel nach:

- Alter
- Geschlecht
- Sprache
- Herkunft
- Kultur
- Religion
- Behinderung
- Bildungsweg

- Erfahrung

Gender-Neutralität bedeutet, Menschen unabhängig vom Geschlecht fair und respektvoll anzusprechen.

Beispiele

Nicht optimal	Besser
Mitarbeiter	Beschäftigte
Ansprechpartner	Ansprechperson
Teilnehmer	Teilnehmende
jeder Benutzer	jede Person / alle Nutzenden

Merksatz

Diversity bedeutet: Unterschiede respektieren und fair berücksichtigen.

---

15. Würde und Integrität von Menschen

Würde und Integrität bedeuten, dass Menschen respektvoll behandelt und nicht verletzt, bloßgestellt oder diskriminiert werden dürfen.

Im digitalen Arbeitsumfeld bedeutet das:

- keine Bloßstellung im Chat
- keine unnötige Überwachung
- keine Diskriminierung durch IT-Systeme
- Schutz persönlicher Daten
- respektvoller Umgang mit Fehlern
- transparente Entscheidungen
- faire Behandlung

Merksatz

Auch digitale Systeme und digitale Kommunikation müssen Menschen respektieren.

Prüfungsfragen zu Kapitel 5

1. Was bedeutet wertschätzende Zusammenarbeit?

Antwort anzeigen

Wertschätzende Zusammenarbeit bedeutet, respektvoll miteinander umzugehen, Beiträge anderer anzuerkennen, sachlich zu kommunizieren und gemeinsam Verantwortung für gute Zusammenarbeit zu übernehmen.

---

2. Was bedeutet Interdisziplinarität?

Antwort anzeigen

Interdisziplinarität bedeutet, dass Menschen aus unterschiedlichen Fachbereichen zusammenarbeiten und ihr Fachwissen gemeinsam in eine Aufgabe einbringen.

---

3. Was bedeutet Interkulturalität?

Antwort anzeigen

Interkulturalität bedeutet, dass Menschen mit unterschiedlichen kulturellen Hintergründen zusammenarbeiten und respektvoll mit unterschiedlichen Erfahrungen, Werten und Kommunikationsweisen umgehen.

---

4. Was bedeutet verantwortungsvoller Umgang mit digitalen Medien?

Antwort anzeigen

Verantwortungsvoller Umgang mit digitalen Medien bedeutet, digitale Medien bewusst, sicher, respektvoll und rechtlich korrekt zu nutzen.

---

5. Warum sind Persönlichkeitsrechte bei digitaler Zusammenarbeit wichtig?

Antwort anzeigen

Persönlichkeitsrechte schützen Privatsphäre, Würde und persönliche Daten. Digitale Inhalte wie Fotos, Screenshots oder personenbezogene Informationen dürfen nicht unbedacht gespeichert oder weitergegeben werden.

---

6. Nenne drei informationstechnische Schutzziele.

Antwort anzeigen

Drei wichtige Schutzziele sind Vertraulichkeit, Integrität und Verfügbarkeit.

---

7. Was bedeutet Vertraulichkeit?

Antwort anzeigen

Vertraulichkeit bedeutet, dass Informationen nur für berechtigte Personen zugänglich sind.

---

8. Was bedeutet Integrität?

Antwort anzeigen

Integrität bedeutet, dass Informationen vollständig und unverändert bleiben und nicht unbemerkt manipuliert werden.

---

9. Was bedeutet Verfügbarkeit?

Antwort anzeigen

Verfügbarkeit bedeutet, dass Informationen, Systeme und Dienste bei Bedarf nutzbar sind.

---

10. Warum ist Authentizität wichtig?

Antwort anzeigen

Authentizität ist wichtig, damit geprüft werden kann, ob Absender, Nutzer oder Systeme wirklich echt sind.

---

11. Was bedeutet Netiquette?

Antwort anzeigen

Netiquette bedeutet höfliche und angemessene Umgangsformen in digitaler Kommunikation.

---

12. Warum muss man Adressatenlisten sorgfältig prüfen?

Antwort anzeigen

Weil vertrauliche oder personenbezogene Informationen sonst an falsche oder zu viele Personen gelangen können.

---

13. Warum kann „Allen antworten“ problematisch sein?

Antwort anzeigen

Weil Informationen dadurch an Personen gelangen können, die diese nicht benötigen oder nicht erhalten dürfen.

---

14. Warum können Äußerungen über den Arbeitgeber in sozialen Netzwerken problematisch sein?

Antwort anzeigen

Weil sie interne Informationen, Kundendaten, Geschäftsgeheimnisse oder beleidigende Aussagen enthalten können. Das kann arbeitsrechtliche oder juristische Folgen haben.

---

15. Was ist Social Engineering?

Antwort anzeigen

Social Engineering ist eine Angriffsmethode, bei der Menschen manipuliert werden, um Informationen, Zugangsdaten oder bestimmte Handlungen zu erhalten.

---

16. Nenne drei Warnzeichen für Social Engineering.

Antwort anzeigen

Warnzeichen sind zum Beispiel ungewöhnlicher Zeitdruck, Bitte um Passwörter, verdächtige Links, unbekannte Absender, Drohungen oder die Aufforderung, Regeln zu umgehen.

---

17. Was bedeutet Compliance?

Antwort anzeigen

Compliance bedeutet, dass sich Unternehmen und Beschäftigte an Gesetze, Vorschriften, interne Regeln und ethische Grundsätze halten.

---

18. Nenne drei Beispiele für Compliance im IT-Bereich.

Antwort anzeigen

Beispiele sind Datenschutzregeln einhalten, nur lizenzierte Software verwenden, Passwortrichtlinien beachten, Zugriffsrechte nicht missbrauchen und Sicherheitsvorfälle melden.

---

19. Warum ist nicht alles, was technisch möglich ist, automatisch erlaubt oder sinnvoll?

Antwort anzeigen

Weil technische Möglichkeiten rechtliche, ethische oder soziale Probleme verursachen können, zum Beispiel Datenschutzverstöße, Überwachung, Diskriminierung oder Verletzung von Persönlichkeitsrechten.

---

20. Was bedeutet Diversity?

Antwort anzeigen

Diversity bedeutet Vielfalt. Im Betrieb meint das unterschiedliche Eigenschaften, Erfahrungen und Hintergründe von Menschen.

---

21. Warum ist Diversity bei IT-Lösungen wichtig?

Antwort anzeigen

Weil IT-Lösungen von unterschiedlichen Menschen genutzt werden. Sie sollten möglichst fair, verständlich, barrierearm und diskriminierungsfrei gestaltet sein.

---

22. Was bedeutet Gender-Neutralität?

Antwort anzeigen

Gender-Neutralität bedeutet, Menschen unabhängig vom Geschlecht fair und respektvoll anzusprechen und niemanden unnötig auszuschließen.

---

23. Nenne ein Beispiel für eine genderneutrale Formulierung.

Antwort anzeigen

Zum Beispiel „Beschäftigte“ statt „Mitarbeiter“ oder „Ansprechperson“ statt „Ansprechpartner“.

---

24. Warum kann dauerhafte Mitarbeiterüberwachung ethisch problematisch sein?

Antwort anzeigen

Sie kann Persönlichkeitsrechte verletzen, Vertrauen zerstören, psychischen Druck erzeugen und unverhältnismäßig sein.

---

25. Warum können IT-Systeme diskriminieren?

Antwort anzeigen

IT-Systeme können diskriminieren, wenn sie mit einseitigen oder fehlerhaften Daten arbeiten, bestimmte Gruppen ausschließen oder Entscheidungen nicht fair und nachvollziehbar treffen.

Kurztest ohne Hilfe

Beantworte diese Fragen ohne nachzuschauen:

- Was bedeutet wertschätzende Zusammenarbeit?
- Was ist Interdisziplinarität?
- Was ist Interkulturalität?
- Welche digitalen Medien werden im Betrieb genutzt?
- Warum sind Persönlichkeitsrechte wichtig?
- Was bedeuten Vertraulichkeit, Integrität und Verfügbarkeit?
- Was ist Netiquette?
- Warum sind Adressatenlisten kritisch?
- Was ist Social Engineering?
- Was bedeutet Compliance?
- Warum ist Überwachung am Arbeitsplatz problematisch?
- Was bedeutet Diversity?
- Was bedeutet Gender-Neutralität?
- Warum müssen IT-Systeme fair und diskriminierungsfrei gestaltet werden?

Merksätze für Kapitel 5

- Wertschätzende Zusammenarbeit = respektvoll, fair und verantwortungsvoll arbeiten.
- Interdisziplinarität = Zusammenarbeit verschiedener Fachbereiche.
- Interkulturalität = respektvoller Umgang mit kulturellen Unterschieden.
- Digitale Medien müssen bewusst, sicher und rechtlich korrekt genutzt werden.
- Persönlichkeitsrechte schützen Würde, Privatsphäre und persönliche Daten.
- Vertraulichkeit = nur Berechtigte sehen Informationen.
- Integrität = Informationen bleiben korrekt.
- Verfügbarkeit = Systeme und Informationen sind nutzbar.
- Authentizität = Echtheit von Absendern, Nutzern oder Systemen.
- Netiquette = höfliche digitale Umgangsformen.
- Adressatenlisten vor dem Senden prüfen.
- Social Engineering manipuliert Menschen.
- Compliance = Regeln einhalten.
- Technisch möglich heißt nicht automatisch erlaubt.
- Diversity = Vielfalt respektieren.
- Gender-Neutralität = fair und respektvoll formulieren.

- Würde und Integrität von Menschen müssen auch digital geschützt werden.