Vernetztes Zusammenarbeiten

Inhalt

- Wertschätzende Zusammenarbeit
- Informationstechnische Schutzziele
- Ethische Aspekte

Übersicht

Wertschätzende Zusammenarbeit

- Wertschätzende Zusammenarbeit
- Interdisziplinarität und Interkulturalität

Wertschätzende Zusammenarbeit

Fähigkeit, effektiv, integer und respektvoll mit verschiedenen Teams zusammenzuarbeiten

Übernahme gemeinsamer Verantwortung für die Zusammenarbeit und Wertschätzung der einzelnen Beiträge jedes Teammitglieds

Unternehmenswerte beachten und betriebliche Ethikregeln anwenden

Interdisziplinarität und Interkulturalität

INTERDISZIPLINARITÄT

- Zusammenarbeit von Personen aus unterschiedlichen **Fachrichtungen** oder **Disziplinen**, um komplexe Aufgaben oder Projekte ganzheitlich zu lösen
- **Beispiel:**
  Ein IT-Projektteam besteht aus Softwareentwicklern, Designern, Betriebswirten und Marketingfachleuten, die gemeinsam an einer App arbeiten
- **Ziele:**
  - Nutzung verschiedener Perspektiven und Fachkompetenzen
  - Förderung von Innovation und Problemlösungskompetenz

INTERKULTURALITÄT

- Zusammenarbeit und Kommunikation zwischen Menschen unterschiedlicher **kultureller Hintergründe**, Werte, Sprachen und Arbeitsstile
- **Beispiel:**
  Ein internationales IT-Team arbeitet online an einem globalen Projekt – kulturelle Unterschiede müssen berücksichtigt werden (z. B. Kommunikationsstile, Feiertage, Entscheidungsprozesse)
- **Ziele:**
  - Förderung gegenseitigen Verständnisses
  - Verbesserung der Teamarbeit in internationalen Strukturen
  - Nutzung kultureller Vielfalt als Stärke

Übersicht

Informationstechnische Schutzziele

- Gefahren im privaten Kontext
- Gefahren im beruflichen Kontext
- Schutzmaßnahmen und Prävention
- Net(t)iquette
- Äußerungen über den eigenen Arbeitgeber in sozialen Netzwerken
- Relevante Gesetze
- Arbeitsrechtliche Folgen
- Social Engineering

Gefahren im privaten Kontext

Gefahrenquelle	Beschreibung	Mögliche Folgen
Datenpreisgabe / Oversharing	Nutzer geben zu viele persönliche Informationen preis, die missbraucht werden können	Identitätsdiebstahl, Social Engineering, Einbruch während Abwesenheit
Phishing & Social Engineering	Kriminelle nutzen soziale Netzwerke, um an Passwörter oder Zugangsdaten zu gelangen	Kontoübernahme, Datenverlust
Malware & Fake-Apps	Schadsoftware verbreitet sich über Links, Werbung oder gefälschte Profile	Virenbefall, Datenverschlüsselung (Ransomware)
Identitätsdiebstahl	Erstellung gefälschter Profile mit fremden Fotos und Daten	Rufschädigung, Betrug, Missbrauch persönlicher Daten
Unzureichende Privatsphäre-Einstellungen	Standard-Einstellungen erlauben weite Sichtbarkeit von Beiträgen	Unbefugte Datennutzung, Mobbing, Doxing
Unbedachte Posts	Aussagen oder Bilder, die später negative Folgen haben können	Abmahnung, Kündigung, Reputationsverlust

Gefahren im beruflichen Kontext

Gefahrenquelle	Beschreibung	Mögliche Folgen
Veröffentlichung vertraulicher Informationen	Mitarbeitende posten versehentlich sensible Firmendaten	Geheimnisverrat, Wettbewerbsnachteil
Social Engineering gegen Unternehmen	Angreifer nutzen Social Media zur Informationsbeschaffung über Mitarbeitende	Gezielte Phishing-Angriffe (Spear Phishing)
Unkontrollierte Kommunikation	Private Meinungen werden mit Unternehmensmeinungen verwechselt	Imageschäden, Reputationsverlust
Datenschutzverstöße	Veröffentlichung personenbezogener Daten ohne Einwilligung	Verstoß gegen DSGVO, Bußgelder
Malware über Social Media-Kanäle	Schadsoftware gelangt über Nachrichten oder Werbung ins Firmennetzwerk	IT-Ausfälle, Datenverlust
Fremdzugriff auf Firmenaccounts	Schwache Passwörter oder fehlende 2-Faktor-Authentifizierung	Imageverlust, Missbrauch der Marke
Fehlende Social-Media-Policy	Keine klaren Regeln für Mitarbeitende zur Nutzung sozialer Medien	Reputationsrisiken, rechtliche Probleme

Schutzmaßnahmen und Prävention

- Social-Media-Richtlinien (Policy)
- Schulung der Mitarbeitenden
- Technischer Schutz
- Datensparsamkeit
- Privatsphäre-Einstellungen
- Sichere Accounts
- Trennung privat / beruflich
- Regelmäßige Kontrolle von Accounts

Net(t)iquette

Eine **Netiquette** (zusammengesetzt aus *Net* = Internet und *Etiquette* = Verhaltensregeln) bezeichnet die **allgemeinen Benimm- und Kommunikationsregeln im digitalen Raum**. Sie legt fest, **wie man sich im Internet oder bei der digitalen Zusammenarbeit respektvoll, klar und verantwortungsbewusst verhält** – sowohl im privaten als auch im beruflichen Kontext.

Ziele:

- freundliches und respektvolles Miteinander im Netz sicherstellen
- Missverständnisse und Konflikte vermeiden
- Kommunikationskultur in digitalen Medien fördern

Net(t)iquette - Grundregeln

Regel	Beschreibung
Respektvoller Umgang	Andere Meinungen akzeptieren und niemanden beleidigen oder provozieren.
Freundlicher Tonfall	Auch schriftlich höflich und sachlich bleiben – Ironie oder Sarkasmus können leicht missverstanden werden.
Klare und verständliche Sprache	Kurz, präzise und verständlich schreiben – Großbuchstaben wirken wie Schreien.
Kritik sachlich äußern	Kritik begründen und lösungsorientiert formulieren.
Keine Diskriminierung oder Beleidigung	Keine Aussagen, die andere aufgrund von Herkunft, Geschlecht, Religion etc. verletzen.
Privatsphäre wahren	Persönliche oder vertrauliche Daten anderer nicht veröffentlichen.
Urheberrechte respektieren	Keine fremden Texte, Bilder oder Musik ohne Erlaubnis verwenden.
Keine Spammails oder Werbung	Keine unerwünschten Massen-Nachrichten oder Eigenwerbung verschicken.
Korrektes Verhalten in Gruppen & Meetings	Auf Redezeiten achten, andere ausreden lassen, Mikrofon stummschalten, wenn man nicht spricht.
Verantwortungsbewusster Umgang mit Emojis & Humor	Emojis sparsam einsetzen, keine doppeldeutigen Symbole oder Inhalte posten.

Äußerungen über den eigenen Arbeitgeber in sozialen Netzwerken

- Äußerungen über den eigenen Arbeitgeber in sozialen Netzwerken können – je nach Inhalt – **arbeitsrechtliche, zivilrechtliche und sogar strafrechtliche Folgen** haben.

Art der Konsequenz	Beschreibung	Mögliche Folgen
Arbeitsrechtliche Konsequenzen	Verstöße gegen arbeitsvertragliche Pflichten	Abmahnung, ordentliche oder fristlose Kündigung
Zivilrechtliche Konsequenzen	Verletzung des Persönlichkeitsrechts oder Unternehmensimages	Schadensersatz- oder Unterlassungsklage
Strafrechtliche Konsequenzen	Verstöße gegen Strafgesetze wie Beleidigung (§ 185 StGB) oder Verleumdung (§ 187 StGB)	Geldstrafe oder Freiheitsstrafe bis zu 2 Jahren
Datenschutzrechtliche Konsequenzen	Veröffentlichung personenbezogener oder betrieblicher Daten ohne Einwilligung	DSGVO-Verstoß, Bußgelder, Schadensersatzforderungen
Reputationsschaden	Negative Wirkung auf das eigene berufliche Image	Vertrauensverlust, Karriereeinbußen, Rufschädigung

Relevante Gesetze

Art. 5 GG

- Meinungsfreiheit – mit Schranken durch allgemeine Gesetze und Persönlichkeitsrechte

§ 241 Abs. 2 BGB

- Rücksichtnahmepflicht im Arbeitsverhältnis

§§ 185–187 StGB

- Beleidigung, üble Nachrede, Verleumdung

§ 823 BGB

- Schadensersatz bei Verletzung des Persönlichkeitsrechts

DSGVO, § 26 BDSG

- Schutz personenbezogener Daten im Arbeitsverhältnis

§ 17 UWG

- Verbot der Verletzung von Betriebs- und Geschäftsgeheimnissen

Arbeitsrechtliche Folgen

Abmahnung:

- Bei einmaligen oder geringfügigen Verstößen – z. B. unsachlichen Kommentaren – erfolgt meist eine Abmahnung

Ordentliche Kündigung:

- Wenn trotz Abmahnung wiederholt beleidigende oder rufschädigende Äußerungen gepostet werden

Fristlose Kündigung:

- Bei schweren Fällen, z. B. Veröffentlichung interner Informationen, grobe Beleidigungen oder falsche Anschuldigungen gegen den Arbeitgeber

Social Engineering

Versuch, durch Täuschung, Vertrauen oder Druck psychologische Schwachstellen von Personen auszunutzen, um an sensible Daten oder Zugangsinformationen zu gelangen

Typische Ziele:			
Passwörter oder Zugangsdaten	interne Dokumente oder Systeme	finanzielle Transaktionen	vertrauliche Informationen über Personen/Unternehmen

Psychologische Manipulationstechniken

Autorität	• Täter gibt sich als Vorgesetzter oder Experte aus
Zeitdruck	• Opfer wird zur schnellen Handlung gedrängt
Hilfsbereitschaft	• Täter nutzt natürliche Kooperationsbereitschaft aus
Neugier / Gier	• Opfer wird mit verlockenden Angeboten oder Informationen gelockt
Angst / Drohung	• Opfer wird eingeschüchtert
Sympathie	• Täter gewinnt Vertrauen durch freundliches, verbindliches Auftreten

Social Engineering - Prävention

- Sensibilisierung und Schulung
- Keine Weitergabe vertraulicher Informationen
- Überprüfung von Identitäten
- Technische Schutzmaßnahmen
- Sicherheitskultur fördern
- Skepsis bei ungewöhnlichen Anfragen

Übersicht

Ethische Aspekte

- Diversity
- Gender-Neutralität
- FLINTA* und LGBTAQI+
- Menschenwürde und Integrität
- Compliance-Regelungen

Diversity

- Vielfalt der Menschen in allen Dimensionen anerkennen und aktiv einbeziehen
- **Ziel:**
  - Gleichbehandlung und faire Chancen für alle Beschäftigten
  - unabhängig von persönlichen Merkmalen

- **Bedeutung im Unternehmen:**
  - Vielfältige Teams sind kreativer, innovativer und erfolgreicher
  - Unterschiedliche Perspektiven führen zu besseren Problemlösungen
  - Diversity ist Teil der Unternehmenskultur und wird häufig in Leitbildern oder Kodizes verankert

Gender-Neutralität

- geschlechtergerechte Sprache, Formulare, IT-Systeme und Arbeitsumgebungen gestalten, damit sich **alle Geschlechter** angesprochen fühlen

Nach dem **Beschluss des Bundesverfassungsgerichts (2017)** muss neben „männlich“ und „weiblich“ auch ein **drittes Geschlecht** (z. B. „divers“) berücksichtigt werden.

- **Praktische Umsetzung:**
  - Verwendung neutraler Formulierungen (z. B. „Mitarbeitende“ statt „Mitarbeiter“)
  - Anpassung von Personalformularen und IT-Systemen
  - Sensibilisierung in Kommunikation, Personalplanung und Führung

FLINTA* und LGBTAQI+

FLINTA*

- **Akronym für :**
  - **F**rauen
  - **L**esben
  - **I**ntergeschlechtliche
  - **N**ichtbinäre
  - **T**ransgeschlechtliche
  - **A**gender Personen
  - * als Platzhalter für alle Personen, die sich in keinem der Buchstaben wiederfinden und aufgrund ihrer geschlechtlichen Identität von Marginalisierung betroffen sind

LGBTAQI+

- **Akronym für :**
  - **L**esbian
  - **G**ay
  - **B**isexual
  - **T**ransgender
  - **A**sexuelle, **A**romantische und **A**gender Personen
  - **Q**ueer
  - **I**ntergeschlechtliche
  - **+** als Platzhalter für alle Personen, die sich in keinem der Buchstaben wiederfinden und aufgrund ihrer geschlechtlichen Identität von Marginalisierung betroffen sind

Menschenwürde und Integrität

GRUNDPRINZIP
Jeder Mensch besitzt eine unveräußerliche Würde – sie zu achten und zu schützen ist oberste Pflicht (Art. 1 GG)

BEDEUTUNG IN DER DIGITALEN WELT

- IT-Systeme und digitale Lösungen müssen so gestalten, dass sie die Integrität und Rechte aller Beteiligten wahren
- Daten dürfen nicht missbraucht, Menschen nicht überwacht oder diskriminiert werden
- Entscheidungen, die auf Algorithmen beruhen, sollten nachvollziehbar und fair sein

ZEITHORIZONT

- **Kurzfristig:** Schutz persönlicher Daten und Wahrung der Privatsphäre
- **Mittelfristig:** Gerechte, transparente Verfahren und Bewertungen
- **Langfristig:** Vertrauensvolle, ethisch fundierte digitale Arbeitskultur

Compliance-Regelungen

- Rechtskonformität und Einhaltung von Gesetzen, Richtlinien und unternehmensinternen Verhaltensregeln durch das Unternehmen und seine Mitarbeitenden sowie „Integrität, Redlichkeit und Geschäftsethik“

Typische Regelungen

- Verhaltenskodex (Code of Conduct)
- Richtlinie zur Gleichberechtigung
- Richtlinie zur Gesundheit und Sicherheit am Arbeitsplatz
- Richtlinie zur Nutzung von Social Media und Internet
- Datenschutzrichtlinie
- Richtlinie zur Regelung von Arbeitszeiten, Abwesenheiten, Urlaub
- Informationssicherheit (IT-Sicherheitsgesetz)
- Arbeitsschutz
- Nachhaltigkeits- und Umweltauflagen