STAR COOPERATION®

Your Partners in Excellence

Richtlinien

Informationssicherheits-Richtlinie für externen Dienstleister und Geschäftspartner

Geltungsbereich: Externe Dienstleister

Stand: 06.10.2025
Version: 5

Inhaltsverzeichnis

1 Präambel

Informationen – unabhängig ob digital oder in sonstiger Form wie Papier - gehören zu unseren wichtigsten Unternehmenswerten. Informationen über Projekte, Finanzen, Geschäftsprozesse, Kunden, Lieferanten, Partner und Mitarbeiter sind unerlässlich für unseren Geschäftserfolg. Deshalb sind der Schutz und die Sicherung dieser Informationen von entscheidender Bedeutung für unser Unternehmen und unsere Kundenbeziehungen.

Um diese Informationen zu schützen und Ihnen eine Hilfestellung beim Umgang mit diesen zu geben, haben wir die nachfolgende Richtlinie erstellt.

1.1 Geltungsbereich

Diese Richtlinie gilt für alle externen Personen (z.B. Dienstleister, Lieferanten, Kunden und an der Projektarbeit beteiligte Personen), die in unserem Unternehmen tätig sind oder Zugang zu unseren Unternehmenssystemen haben. Die externen Personen sind verpflichtet, sich an diese Richtlinie zu halten. Zur Sicherstellung der durchgängigen Informationssicherheit bedarf ein Abweichen von den Vorgaben dieser Richtlinie der schriftlichen Zustimmung des Informationssicherheitsbeauftragten.

1.2 Einhaltung von Rechtsvorschriften

Bei Umgang mit Informationen in unserem Unternehmen sind von den externen Personen die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit sowie die Unternehmensregelungen einzuhalten. Sollten externe Personen unsicher sein, ob und inwieweit Rechtsvorschriften oder Unternehmensregelungen einzuhalten sind, haben sie sich an ihren unternehmensinternen Ansprechpartner zur Klärung zu wenden. Dieser muss ggf. Unklarheiten mit der IT-Abteilung, dem Informationssicherheits- oder Datenschutzbeauftragten abstimmen.

2 Verwenden von Anmeldeinformationen

Zur Sicherstellung eines ausreichenden Zugangs- und Zugriffsschutzes ist es zwingend erforderlich, dass die Zugangsberechtigten mit Zugang zu den Datenverarbeitungssystemen sichere Passwörter verwenden. Jeder Zugangsberechtigte des Datenverarbeitungssystems erhält einen ihm zugeordneten, eindeutigen Benutzernamen, mit dem der Nutzende am jeweiligen Datenverarbeitungssystems identifiziert wird. Die nachfolgenden Passwort-Regelungen sind daher unbedingt von jedem Zugangsberechtigten einzuhalten:

- Startpasswörter, die die Zugangsberechtigten im Rahmen der ersten Anmeldung erhalten, sind umgehend durch eigene (individuelle) Passwörter zu ersetzen
- Passwörter dürfen nicht aufgeschrieben oder am Arbeitsplatz hinterlegt werden
- Passwörter dürfen nicht an Dritte (auch Kollegen der Abteilung) weitergegeben werden
- Eine Anmeldung mit den Anmeldedaten eines anderen Benutzers ist verboten
- Bei der Eingabe von Passwörtern ist darauf zu achten, dass Dritte Passwörter nicht zur Kenntnis nehmen
- Mindestlänge des Passworts sind 14 Zeichen
- Passwörter müssen mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer oder ein Sonderzeichen enthalten
- Trivialpasswörter dürfen nicht verwendet werden (z.B. Benutzername, Oktober2024, qwertz, 12345678, abcdefg)
- Das Geburtsdatum des Benutzers oder dessen Angehörigen darf nicht als Passwort verwendet werden
- Passwörter müssen regelmäßig selbstständig vom Benutzer gewechselt werden, Sie werden hierzu automatisch nach 12 Monaten zur Neuvergabe eines Kennworts aufgefordert, bzw. sind auf Verlangen

des Informationssicherheitsbeauftragten/Anwenderbetreuung bspw. bei Verdacht einer Kompromittierung, sofort zu wechseln
- Passwörter dürfen ohne entsprechende Schutzmechanismen nicht in dem Datenverarbeitungssystem (bspw. in einem Internet-Browser) gespeichert werden
- Die innerhalb des Unternehmens (Netzwerk) verwendeten Passwörter dürfen nicht für Anwendungen im Internet oder im privaten Umfeld verwendet werden

3 Verwenden von Kommunikationsmitteln

3.1 Mailsystem

Sofern Ihnen eine E-Mail-Account zur Verfügung gestellt wird, darf dieser ausschließt für die geschäftliche Kommunikation der STAR COOPERATION Unternehmensgruppe verwendet werden. Eine private Nutzung ist ausdrücklich verboten.

Automatische E-Mail-Weiterleitungen / forwards an externe Verarbeitungssysteme/Dritte ist untersagt.

Bei allen geschäftlichen Nachrichten, die Nutzende per E-Mail veröffentlichen oder weitergeben, muss klar erkennbar sein, welche Person für den Inhalt verantwortlich ist. Das Versenden von geschäftlichen E-Mails muss immer mit Signatur erfolgen.

3.1.1 Schutz vor Bedrohungen bei der E-Mail-Nutzung

Beachten Sie vor dem Öffnen jeder E-Mail, Absender, Betreff und Anhang.

- Ist der Absender bekannt?
- Ist der Betreff sinnvoll?
- Wird ein Anhang von diesem Absender erwartet?

In Kombination liefern diese Fragen einen guten Anhaltspunkt, um eine E-Mail als vertrauenswürdig einzustufen.

Merkmale von Bedrohungs-Mails:

- Vage Formulierung im Betreff, wie bspw. „Rechnung“, „Mahnung“ oder „Dringende Nachricht“.
- Die Absender-E-Mail-Adresse enthält ungewöhnliche Bestandteile oder Buchstabenkombinationen. Technische Details „Internetkopfzeilen“ können bei einer geöffneten E-Mail über „Datei“ – „Eigenschaften“ eingesehen werden.
- Oft keine persönliche Anrede vorhanden. Oftmals Rechtschreibfehler enthalten.
- Es wird nach vertraulichen Daten wie Passwörter/Anmeldeinformationen oder Kontodaten gefragt.
- Hinweis auf dringenden Handlungsbedarf oder Einhaltung von Fristen.
- Enthaltene Links wirken auf den ersten Blick echt, enthalten jedoch ungewöhnliche oder falsch geschrieben Bestandteile.

E-Mails, die den oben genannten Merkmalen entsprechen, sollen bitte an Ihren unternehmensinternen Ansprechpartner/Repräsentanten gemeldet werden.

3.1.2 Schutz vor unverlangter Werbung (Spam)

Zum Schutz vor unverlangter Werbung durch E-Mail werden im Unternehmen so genannte Spam-Filter eingesetzt. Der Einsatz des Spam-Filters erfolgt aus betrieblichen Gründen. Durch den Spam-Filter kann es dazu kommen, dass E-Mails automatisch in den Ordner „Junk-E-Mail“ verschoben werden und nach 30 Tagen gelöscht werden.

3.2 Internet

Der „Download“ von Dateien, Programmen und urheberrechtlich geschützten Bildern aus dem Internet ist verboten. Ausgenommen von diesem Verbot ist das Öffnen und Speichern von geschäftlichen PDF- und Office-Dateien aus vertrauenswürdigen Quellen.

Bei allen geschäftlichen Nachrichten, die Nutzende über lokale, nationale oder internationale Netze veröffentlichen oder weitergeben (z.B. durch Web- Pages, FTP, Usenet- News etc.), muss klar erkennbar sein, welche Person für den Inhalt verantwortlich ist.

Speichern sie die Zugangsdaten zu den Unternehmenssystemen nicht in Ihrem Browser.

3.3 Soziale Netzwerke

Die Nutzung von sozialen Netzwerken wie bspw. XING, LinkedIn, Facebook oder ähnliche, birgt Gefahren wie Verlust von Ansehen, Belästigung und Mobbing, Verbreitung von Viren und Malware, Verlust von Geschäftsgeheimnissen, Überwachung von Mitarbeitern durch externe Personen, Erpressung oder Identitätsdiebstahl.

Daher ist der verantwortungsvolle Umgang damit von elementarer Bedeutung.

- Geben Sie keine firmeninternen Informationen oder Informationen über Kundenprojekte preis.
- Persönliche Profile dürfen keine Zusätze wie „arbeitet zurzeit für Kunde XXXX“ oder ähnliches enthalten.
- Mit Informationen, die Sie von Dritten erhalten, sollten mit Vorsicht und einem gesunden Misstrauen umgegangen werden, da diese möglicherweise gar nicht von der Person stammen, für die sich der Absender ausgibt.
- Die Datensparsamkeit, bzw. das Einstellen möglichst weniger persönlicher Informationen ist ein Grundprinzip im sicheren Umgang mit sozialen Netzwerken.
- Beachten Sie, dass bei Kommunikation in sozialen Netzwerken auch eine Verbindung mit dem Unternehmen hergestellt werden kann. Daher sollte auf eine angemessene Ausdrucksweise geachtet werden.

Grundsätzlich gilt:
Verhalten Sie sich in sozialen Netzwerken den Mitgliedern gegenüber so, wie Sie es auch im realen Leben tun würden.

3.4 Künstliche Intelligenz (KI)

Die Nutzung von Microsoft Copilot und Copilot Chat ist für den geschäftlichen Einsatz vorgesehen und erfolgt im Rahmen der bereitgestellten und abgesicherten STAR-Infrastruktur und kann für jegliche Art von Recherche verwendet werden.

Im Gegensatz dazu ist bei der Nutzung von KI-basierten Anwendungen außerhalb der STAR-Infrastruktur, wie z. B. ChatGPT oder vergleichbaren Systemen, ist sicherzustellen, dass sämtliche Anforderungen an die Informationssicherheit sowie den Datenschutz gemäß geltenden gesetzlichen und unternehmensinternen Vorgaben eingehalten werden. Insbesondere dürfen keine vertraulichen, personenbezogenen oder geschäftskritischen Informationen in externe KI-Systeme eingegeben werden, sofern keine explizite Freigabe durch die zuständigen Stellen erfolgt ist.

Folgende Eingaben (Input) sind unzulässig:

- Als intern, vertraulich und geheim eingestufte Informationen. (bei nicht freigegebener Nutzung)
- Sicherheitsrelevante Informationen, z.B. Kennwörter oder Zugangsdaten.

- Urheberrechtlich geschützte Informationen, an denen die STAR-Unternehmensgruppe keine entsprechenden Nutzungsrechte besitzt.

Verwendungseinschränkungen für das Ergebnis (Output):

- Der Dienst kann ungenaue Informationen über Personen, Orte oder Fakten darstellen, die fachliche und sachliche Korrektheit ist vor Verwendung zu dienstlichen Zwecken zu prüfen.
- Arbeitsergebnisse eines KI-Tools dürfen nicht ohne menschliche Überprüfung einer weiteren Verwendung zugeführt werden. Ungeprüfte Arbeitsergebnisse eines KI-Tools müssen als solche gekennzeichnet werden.
- Der Dienst kann ein Ergebnis (Output) liefern, das unter Umständen einem bereits urheberrechtlich geschützten Text entspricht.

Seien Sie sich im Klaren darüber, dass das Ergebnis (Output) keiner Exklusivität unterliegt und somit auch von Dritten erzeugt werden kann. Zudem weisen die Ergebnisse manchmal eine bestimmte Struktur auf, die von Dritten als bspw. ChatGPT-Output erkannt wird. Es besteht die Möglichkeit, dass in den Antworttexten von ChatGPT eine Art digitales Wasserzeichen (z. B. charakteristische Abfolge von Buchstaben über mehrere Wörter hinweg) enthalten ist, mit dem nachgewiesen werden kann, dass der Text mittels ChatGPT erstellt wurde. Eine Kennzeichnung der mithilfe von bspw. ChatGPT erzeugten Texte schafft Transparenz und verhindert eine „Enthüllung“ durch Dritte.

3.5 Schutz geistigen Eigentums und Urheberrecht

Bei der Nutzung von Kommunikationsmitteln, IT-Systemen sowie sämtlichen digitalen Ressourcen sind die Urheberrechte sowie sonstige geistige Eigentumsrechte Dritter zwingend zu beachten und einzuhalten.

Die Verwendung urheberrechtlich geschützter Werke (z.B. Bilder, Musik, Videos, Texte, Software, Logos, Marken, Präsentationen) ist nur zulässig, wenn:

- eine gültige Lizenz oder ausdrückliche Genehmigung des Rechteinhabers vorliegt,
- die Werke wurden von Arbeitnehmern des Unternehmens selbst erstellt und das Unternehmen ist Nutzungsberechtigter
- die Nutzung ist durch eine gesetzliche Schrankregelung ausdrücklich gestattet.

Bei Unsicherheiten hinsichtlich der Rechtslage oder Lizensierung ist vor der Nutzung die zuständige Fachabteilung (z.B. Rechtsabteilung oder Anwenderbetreuung) einzubeziehen.

Verstöße gegen diese Bestimmung könnten arbeits- und zivilrechtliche Konsequenzen nach sich ziehen.

4 Klassifizierung von Informationen

Zur Gewährleistung des sicheren und sorgsamen Umgangs mit Informationen sind die folgenden 4 Kategorien für die Einstufung von Informationen hinsichtlich Vertraulichkeit festgelegt.

- Die Einstufung **geheim** bezeichnet die vertraulichsten aller Informationen gemäß Schutzklasse 3 der DIN 66399 und der Sicherheitsstufen 4, 5, 6 und 7. Die Weitergabe von geheimen Informationen muss auf einen sehr kleinen, namentlich bekannten Kreis von Personen beschränkt sein.
  - Geheime Informationen sind immer unter Verschluss zu halten
  - Papierunterlagen sind mit dem Wort „Geheim“ zu kennzeichnen. Dies kann durch einen Stempel oder ähnliche Kennzeichnungen erfolgen

- Für die Erstellung von geheimen Informationen ist eine spezielle Vorlage (mit Fußzeile „Geheim“) zu verwenden
- Der Versand von geheimen Informationen per Post ist nicht gestattet
- Geheime Informationen dürfen NUR VERSCHLÜSSELT per E-Mail versendet werden
- Das Speichern von geheimen Informationen darf NUR AUF VERSCHLÜSSELTEN Datenträgern erfolgen.
- Die Löschung und Vernichtung, muss in geeigneter Weise erfolgen (Aktenvernichter etc.)

Beispielsweise für **geheim** eingestufte Informationen:

- Strategische Entscheidungsgrundlagen
- Dokumentationen zu gravierenden Störfällen
- Unterlagen zu neuen Entwicklungen, die an externen Dienstleister übermittelt werden

- Die Einstufung **vertraulich** bezeichnet Informationen mit dem zweithöchsten Vertraulichkeitsniveau gemäß Schutzklasse 2 der DIN 66399 und der Sicherheitsstufe 3. Die Weitergabe von vertraulichen Informationen muss auf einen berechtigten Personenkreis beschränkt sein.
  - Vertrauliche Informationen sind immer unter Verschluss zu halten
  - Papierunterlagen sind mit dem Wort „Vertraulich“ zu kennzeichnen. Dies kann durch einen Stempel oder ähnliche Kennzeichnungen erfolgen.
  - Für die Erstellung von vertraulichen Informationen ist eine spezielle Vorlage (mit Fußzeile „Vertraulich“) zu verwenden.
  - Vertrauliche Informationen dürfen NUR VERSCHLÜSSELT per E-Mail versendet werden.
  - Das Speichern von vertraulichen Informationen erfolgt in Dateiverzeichnissen mit eingeschränktem Benutzerzugriff.

  Beispielsweise sind **vertraulich** eingestufte Informationen:

  - Unterlagen, die der Jahresabschlusserstellung dienen
  - Kalkulationen
  - Personalunterlagen
  - Entgelt-Unterlagen
  - Bewerberunterlagen
  - Betriebswirtschaftliche Daten, Reports
  - Vertragsunterlagen
  - Entwicklungsdaten
  - Projektdaten

- **Intern** ist die gebräuchlichste Einstufung von Informationen gemäß Schutzklasse 1 der DIN 66399 und der Sicherheitsstufen 1 und 2. Die Weitergabe von internen Informationen ist normalerweise auf größere Personengruppen beschränkt. Der Versand von E-Mails ist unverschlüsselt möglich. Alle erstellten Dokumente gelten grundsätzlich zunächst als „Intern“ und sind in der Fußzeile der erstellten Dokumente zu kennzeichnen.

  Beispielsweise sind **intern** eingestufte Informationen:

  - Telefonverzeichnis der Mitarbeiter
  - Organigramme
  - Aufgabenbeschreibungen
  - Kundendatenbanken
  - Besprechungsprotokolle

- Als **öffentlich** eingestufte Informationen sind nicht vertraulich und für den allgemeinen Gebrauch innerhalb und außerhalb von STAR bestimmt.

  Beispielsweise sind **öffentlich** eingestufte Informationen:

  - Marketingunterlagen Vertriebspräsentationen
  - Referenzliste
  - Unternehmensbroschüren

Die Verantwortung für die richtige Klassifizierung und dem Umgang mit den Informationen trägt der Informationseigner.

5 Kennzeichnung von Informationen

5.1 Explizite Kennzeichnung

- Sind Informationen explizit zu kennzeichnen, so ist der Träger der Information (z.B. Papierbogen, DVD) deutlich erkennbar mit der entsprechenden Kennzeichnung in der Fußzeile zu versehen.
- Mehrseitige Dokumente in Papier- oder Dateiform sind auf jeder Seite in der Fußzeile zu kennzeichnen, die Gesamtseitenzahl muss erkennbar sein.

5.2 Implizite Kennzeichnung

- Die implizite Kennzeichnung stellt eine Erleichterung für die tägliche Arbeit dar. Die Informationen sind nicht selbst gekennzeichnet. Bearbeiter einer Aufgabe, die bestimmte Informationen regelmäßig nutzen, kennen die Klassifizierung anhand der Art der Informationen.
- Die implizite Kennzeichnung ist maximal für vertrauliche Informationen möglich, solange diese den Aufgabenbereich nicht verlassen.

6 Richtiger Umgang mit schützenswerten Informationen und Endgeräten am Arbeitsplatz

Dienstleister, Lieferanten usw. sind dazu verpflichtet, Informationen, egal ob digital oder in sonstiger Form, gegenüber dritten unberechtigten Personen geheim zu halten.

Geschäftsdaten unterliegen dem Betriebsgeheimnis und sind Eigentum der STAR COOPERATION Unternehmensgruppe. Um diese Daten zu schützen, sind die Punkte in der folgenden Tabelle zur physischen Aufbewahrung von Informationen einzuhalten:

Standort	Informationsklassifizierung			
	Öffentlich	Intern	Vertraulich	Geheim
Allgemein	Keine Einschränkung	Zugriff durch unbefugte Dritte verhindern. Eine angemessene technische Umsetzung ist durch den Informations-verantwortlichen im Einzelfall in Abhängigkeit von den Gefährdungen zu gewährleisten.	Zugriff durch unbefugte Dritte verhindern. Eine angemessene technische Umsetzung ist durch den Informations-verantwortlichen im Einzelfall in Abhängigkeit von den Gefährdungen zu gewährleisten.	Zugriff durch unbefugte Dritte verhindern. Eine angemessene technische Umsetzung ist durch den Informations-verantwortlichen im Einzelfall in Abhängigkeit von den Gefährdungen zu gewährleisten.
In Firmengebäuden der STAR COOPERATION Unternehmens-gruppe	Keine Einschränkung	Besucher oder sonstige Dritte dürfen keinen Zugang zu Informationen erlangen; Clean Desk.	Lassen Sie nie vertrauliche Arbeitsunterlagen unbeaufsichtigt auf Ihrem Schreibtisch liegen. Schließen Sie diese stattdessen in Rollcontainern, Schränken bzw. Tresoren ein.	Lassen Sie nie geheime Arbeitsunterlagen unbeaufsichtigt auf Ihrem Schreibtisch liegen. Schließen Sie diese stattdessen in Rollcontainern, Schränken bzw. Tresoren ein.
Home-Office/Telearbeit/ Unterwegs	Keine Einschränkung	Besucher oder sonstige Dritte (wie Kunden, Familien-angehörige oder Mitreisende) dürfen keinen Zugang zu Informationen erlangen	Lassen Sie nie vertrauliche Arbeitsunterlagen unbeaufsichtigt auf Ihrem Schreibtisch liegen. Schließen Sie diese stattdessen in Rollcontainern, Schränken bzw. Tresoren ein. Auf Reisen sollten nur die notwendigsten Dokumente mitgeführt und entsprechend unter Verschluss gehalten werden.	Lassen Sie nie geheime Arbeitsunterlagen unbeaufsichtigt auf Ihrem Schreibtisch liegen. Schließen Sie diese stattdessen in Rollcontainern, Schränken bzw. Tresoren ein. Auf Reisen sollten nur die notwendigsten Dokumente mitgeführt und entsprechend unter Verschluss gehalten werden.

Der Arbeitsplatz ist so zu gestalten, dass Besucher oder sonstige Dritte keinen Zugang zu Informationen erlangen können, ohne hierfür berechtigt zu sein. Geeignete Maßnahmen dies umsetzen sind beispielweise:

- In Bereichen mit Publikumsverkehr sind die IT-Systeme – insbesondere die Bildschirme – so auszurichten oder auszustatten, dass die Einsichtnahme durch Dritte nicht möglich ist.
- Sperren Sie Ihren Computer vor dem Verlassen des Arbeitsplatzes (Tasten "Strg+ALT+Entf" drücken und dann auf "Computer sperren" klicken), oder beenden Sie die Sitzung an Ihrem Computer immer durch "Herunterfahren" und nicht durch "Ruhezustand" oder "Standby". Dies gilt auch bei Home-Office-Arbeitsplätzen.
- Beenden Sie die Verbindung zu den Unternehmenssystemen, sobald Sie Ihre Tätigkeit in den Unternehmenssystemen abgeschlossen haben.
- Lassen Sie keine Unterlagen (insbesondere Aufzeichnungen auf Flip-Charts oder Whiteboards etc.) in Besprechungszimmern liegen.
- Lassen Sie nie vertrauliche oder geheime Arbeitsunterlagen unbeaufsichtigt auf Ihrem Schreibtisch liegen. Schließen Sie diese stattdessen in Rollcontainern, Schränken bzw. Tresoren ein.

- Lassen Sie mobile Geräte nicht unbeaufsichtigt. Außerhalb der üblichen Büroarbeitszeiten sind Notebooks mit Kensington-Schlössern abzusichern oder unter Verschluss zu halten.
- Verwahren Sie Handys, Schlüssel, Zugangstokens sicher.
- Es ist nicht gestattet, geschäftliche Daten auf private Datenträger zu speichern (CD-Rom, USB-Stick, etc.)

7 Richtiger Umgang mit schützenswerten Informationen auf Reisen

Auf den genutzten mobilen Endgeräten, (z.B. Laptops, Handys, Smartphones, Tablets, USB-Sticks, ...), sind ggf. unternehmenseigene Daten gespeichert. Verlust oder Diebstahl können schädliche Auswirkungen für Unternehmen haben.

- Nehmen Sie grundsätzlich nur die Unterlagen, die Sie tatsächlich benötigen, mit auf Dienstreisen.
- Speichern Sie nur die Daten lokal verschlüsselt ab, die Sie unterwegs benötigen.
- Benachrichtigen Sie bei Verlust oder Diebstahl mobiler Endgeräte Ihren unternehmensinternen Ansprechpartner/Repräsentanten.
- Führen Sie keine mobilen Endgeräte ohne Passwortschutz mit sich.
- Geben Sie mobile Endgeräte bei Reisen nicht mit Ihrem Koffer auf.
- Lassen Sie mitgeführte Unterlagen und mobile Endgeräte nie unbeaufsichtigt (z.B. im Auto, Bahnhöfen, Flughäfen, Restaurants) liegen. Auch Temperaturschwankungen können nicht nur die Festplatte, sondern auch andere Speichermedien sowie das Display beschädigen.
- Wirtschaftsspionage ist besonders auf Dienstreisen ins Ausland ein Thema. So kann z.B. bei Reisen eine Einsichtnahme/Manipulation durch den Zoll nicht ausgeschlossen werden.
  Beachten Sie die Sicherheits- und Reisehinweise des Auswärtigen Amtes auch in Bezug auf die Informationssicherheit. (https://www.auswaertiges-amt.de/de/ReiseUndSicherheit/reise-und-sicherheitshinweise)
  Bei Verdacht auf Datenverlust und ungewöhnlichen Vorkommnissen, informieren Sie bitte unverzüglich Ihren unternehmensinternen Ansprechpartner/Repräsentanten.

8 Richtiges Verhalten in der Öffentlichkeit und im privaten Umfeld

Viele Geschäftsgeheimnisse werden durch Gedankenlosigkeit vor allem in Gesprächen mit Kollegen oder durch Telefongespräche in öffentlichem oder privatem Umfeld (z.B. Flugzeug, Biergarten, Restaurant) preisgegeben.

- Seien Sie sich immer bewusst, worüber Sie wo kommunizieren. Achten Sie bei allen Gesprächen auf Vertraulichkeit.
- Teilen Sie Informationen in Telefongesprächen nur mit berechtigten Ansprechpartnern.
- Prüfen Sie im Zweifelsfall durch einen Rückruf die Identität des Anrufers.
- Achten Sie unterwegs und im privaten Umfeld darauf, dass niemand einsehen kann, woran Sie arbeiten (z.B. Laptop, Dokumente, etc.).
- Geben Sie keine vertraulichen und geheimen Unternehmensinformationen in privaten Gesprächen preis.
- Führen Sie keine vertraulichen Gespräche in der Öffentlichkeit (z.B. in Flugzeugen, in Hotels, Restaurants).
- Übermitteln Sie keine vertraulichen und geheimen Informationen über Dritte.
- Lassen Sie mobile Endgeräte nie unbeaufsichtigt.
- Halten Sie mobile Endgeräte und Dokumente unter Verschluss, wenn Sie nicht daran arbeiten.
- Geben Sie die Unternehmenshardware nicht an Dritte (auch Familienangehörige) weiter.

9 Richtiges Verhalten in unseren Geschäftsräumen

- Externe Personen müssen Besucherausweise tragen und am Empfang registriert werden.
- Besucherausweise müssen vor dem Verlassen des Gebäudes am Empfang abgegeben werden.
- Die standortbezogenen Sicherheitshinweise müssen eingehalten werden (z.B. Fotografierverbot, Schutzausrüstung usw.).
- Fremdgeräte dürfen nicht an das Unternehmensnetzwerk angeschlossen werden.

10 Verhalten bei Sicherheitsereignissen und -vorfällen

Bei einem **Informationssicherheitsereignis** oder auch **Schwachstelle**, liegt eine mindestens potenziell sicherheitsrelevante Situation oder Verdacht vor, in der noch nicht notwendigerweise ein Schaden für die Organisation und ihre Werte entstanden sein muss, wie zum Beispiel:

- das erkannte Auftreten eines Computervirus, der jedoch unschädlich gemacht werden konnte,
- eine erhaltene Phishing-Nachricht, sofern keine Anmeldeinformationen preisgegeben wurden,
- eine erkannte Verletzung der Zutritts- und Zugriffsregeln und -kontrollen,
- das Nichteinhalten einer Richtlinie durch eine Person, sofern die Verletzung der Richtlinie in diesem Fall keine Folgen für die Informationssicherheit hatte.

Als **Informationssicherheitsvorfälle** werden diejenigen Informationssicherheitsereignisse verstanden, die einzeln oder in Summe zu einer Situation geführt haben oder höchstwahrscheinlich noch führen werden, in der eine Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit von Werten (Informationswerten, IT-Diensten oder -Anwendungen etc.) vorliegt und die zu negativen Folgen für die Organisation führt. Ein konkret feststellbarer und in der Regel messbarer Schaden ist die Konsequenz.

Die Schutzziele für die Informationssicherheit sind:

- **Vertraulichkeit**: Informationen dürfen lediglich von berechtigten Personen während der Dauer ihrer Tätigkeit zugänglich sein.
- **Integrität**: Informationen dürfen nicht unbefugt manipuliert oder geändert werden.
- **Verfügbarkeit**: Informationen stehen für die zugriffsberechtigten Personen verfügbar; Verhinderung von Systemausfällen.

Sollte Sie bemerken, dass der Schutz oder die Sicherheit von Informationen in irgendeiner Weise gefährdet sein könnte, wenden Sie sich unverzüglich an den unternehmensinternen Ansprechpartner/Repräsentanten. Dies gilt insbesondere dann, wenn sich die Gefährdung auf personenbezogene Daten bezieht.

Für die STAR COOPERATION Unternehmensgruppe

Oliver Messer
Aktualisiert Oktober 2025