B to B - Praxistools für Unternehmen und Freiberufler

knowNOW
TOOLS FOR BUSINESS SUCCESS

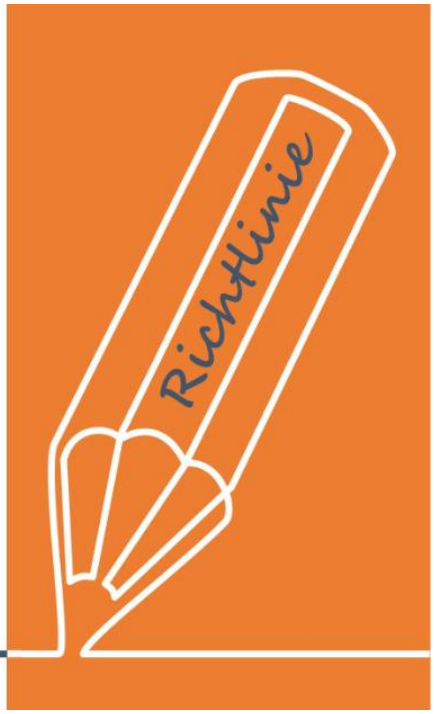
Richtlinie Umgang mit Informationsträgern IT

UseNOW - TeachNOW - LearnNOW - FindNOW

- Sofort nutzbar: Auswählen - Anpassen - Anwenden
- In der Praxis erprobt und bewährt
- Im Tagesgeschäft sofort anwendbare Hilfsmittel
- Aktuell durch regelmäßige Updates

Richtlinie Umgang mit Informationsträgern IT

des Unternehmens



Inhaltsverzeichnis

1. Zweck und Zielsetzung

Diese Richtlinie verfolgt das Ziel, den Umgang mit Informationsträgern in der IT so zu regeln, dass der Schutz und die Vertraulichkeit von Informationen und Daten gewährleistet ist indem klare Vorgaben festgelegt werden. Die Zielsetzung ist, das Risiko von Datenverlust, unbefugtem Zugriff und Informationslecks zu minimieren, indem der gesamte Lebenszyklus von Informationsträgern - von der Nutzung bis hin zur Entsorgung - gesteuert wird.

2. Geltungsbereich

Diese Richtlinie gilt für alle Beschäftigten, Dienstleister und alle anderen relevanten Parteien, die auf die auf sicherheitsrelevante Bereiche unserer IT-Systeme und gespeicherte Informationen Zugriff haben.

3. Verantwortlichkeiten

Beim Umgang mit Informationsträgern in der IT haben wir die folgenden Verantwortlichkeiten festgelegt:

- **Beschäftigte:**
  Jeder Nutzer ist verantwortlich für den sorgsamen und sicheren Umgang mit Informationsträgern, inklusive des Schutzes vor unbefugtem Zugriff und der Einhaltung dieser Richtlinien.
- **IT-Abteilung, IT-Dienstleister:**
  Die IT-Abteilung stellt sicher, dass geeignete technische Maßnahmen und Werkzeuge für den sicheren Umgang mit Informationsträgern verfügbar sind, und ist für die Implementierung von Verschlüsselungs- und Zugriffskontrollsystemen verantwortlich. Externe Partner oder Dienstleister, die mit Informationsträgern in Berührung kommen, müssen vertraglich verpflichtet werden, dieselben Sicherheitsanforderungen einzuhalten wie interne Mitarbeiter.
- **Datenschutzbeauftragter:**
  Er/sie stellt sicher, dass alle Vorgaben zum Datenschutz eingehalten werden, und ist für die Bewertung datenschutzrelevanter Risiken verantwortlich.
- **Informationssicherheitsbeauftragte(r):**
  Er/sie definiert die Sicherheitsanforderungen und Maßnahmen im Umgang mit Informationsträgern, überwacht deren Einhaltung durch regelmäßige Audits und führt Schulungen durch.
- **Vorgesetzte:**
  Sie sind verantwortlich für die Durchsetzung der Richtlinien in ihrem Bereich und für die Aufklärung ihrer Mitarbeiter über die Sicherheitsmaßnahmen und den korrekten Umgang mit Informationsträgern.

Diese klaren Verantwortlichkeiten helfen, den Schutz von Daten zu gewährleisten und eine Sicherheitskultur innerhalb des Unternehmens zu fördern.

4. Schutzbedarf von Informationsträgern

Um den Schutzbedarf von Informationsträgern zu bestimmen und die richtigen Sicherheitsmaßnahmen anzuwenden, sind für Informationsträger die Anforderungen der „*Richtlinie Informationsklassifizierung*“ anzuwenden.

Die folgenden Anforderungen gelten für die Kennzeichnung der Informationsträger:

- Informationsträger mit vertraulichen oder streng vertraulichen Daten sollten gemäß ihrer Klassifikation deutlich gekennzeichnet sein. Dies kann in folgender Form geschehen:
  - Labels auf physischen Datenträgern,
  - Kennzeichnung von Schriftstücken,
  - digital in Metadaten oder
  - mittels Zuordnung in einer Tabelle (siehe Inventarisierung, Punkt 5.).
- Für die Kennzeichnung ist der Ersteller oder Eigentümer der Information verantwortlich.

Die Klassifizierung sollte regelmäßig überprüft und angepasst werden, um sicherzustellen, dass die Einstufung auch im Laufe der Zeit und bei geänderten Rahmenbedingungen noch passend ist.

5. Sichere Aufbewahrung und Lagerung/ Inventarisierung

Informationsträger sollten so gehandhabt werden, dass diese sowohl vor unbefugtem Zugriff als auch vor Umwelteinflüssen geschützt sind und die Integrität der darauf enthaltenen Informationen gewahrt bleibt. Dies umfasst grundsätzlich die folgenden Aspekte:

- Dokumentation und Inventarisierung
  Informationsträger sollten inventarisiert und die Lagerorte dokumentiert werden, um jederzeit nachvollziehen zu können, wo sich welche Informationsträger befinden (bei Bedarf sichere Lagerorte) und wer dafür verantwortlich ist.
- Temperatur- und Umweltschutz:
  Informationsträger, die empfindlich gegenüber Temperatur, Feuchtigkeit oder anderen Umwelteinflüssen sind, sollten in geeigneten Bereichen aufbewahrt werden, um ihre Integrität und Langlebigkeit sicherzustellen.
- Trennung und Kennzeichnung:
  Informationsträger sollten entsprechend ihrer Klassifizierung getrennt und deutlich gekennzeichnet gelagert werden, um Verwechslungen zu vermeiden und sicherzustellen, dass jeder Informationsträger den passenden Schutz erhält.

Für Informationsträger mit der Klassifizierung „vertraulich“ oder „streng vertraulich“ gelten zusätzlich die folgenden Aspekte:

- Verschlüsselung sensibler Daten:
  Diese Informationsträger sollten verschlüsselt werden, um einen Schutz vor unbefugtem Zugriff zu gewährleisten. Dies gilt besonders, wenn die Träger außerhalb gesicherter Umgebungen gelagert werden.

6. Verwendung und Transport von Informationsträgern

Die hier getroffenen Festlegungen sollen dazu beitragen, Informationsträger mit der Klassifizierung „vertraulich" oder „streng vertraulich" während der Verwendung und des Transports stets vor unbefugtem Zugriff und Verlust geschützt bleiben.

- Zugriffsregelung für Medien:
  Informationsträger müssen so aufbewahrt werden, dass nur berechtigte Personen Zugriff haben. Dies kann durch Betriebssysteme, physische Medien, kontrollierte Zugriffsrechte für digitale Medien und eine Zugangskontrolle für Räume, in denen Träger gelagert werden, erreicht werden.
- Verwendung mobiler Endgeräte:
  Bei der Verwendung mobiler Informationsträger oder Geräten außerhalb des Unternehmens sollte darauf geachtet werden, dass die Geräte in gesicherten Umgebungen verwendet werden. Der Zugriff auf offene WLAN-Netzwerke ist ohne besondere Vorkehrungen nicht zulässig, um das Risiko eines unbefugten Zugriffs zu minimieren.
  Weitere Vorgaben enthält die *„Richtlinie mobiles Arbeiten"*.
- Sofortige Meldung von Zwischenfällen:
  Im Fall eines Verlusts oder Diebstahls von Informationsträgern muss dies unverzüglich gemeldet werden, damit die notwendigen Sicherheitsmaßnahmen ergriffen werden können.
- Verpackung und Transport:
  Informationsträger sollten in sicheren und undurchsichtigen Verpackungen transportiert werden, um den Inhalt zu schützen und unbefugtes Einsehen zu verhindern.

7. Löschung und Entsorgung

Datenträger und Akten dürfen nie im üblichen Büroabfall entsorgt werden. Nicht löschbare Akten und Datenträger (z.B. CDs, DVDs, defekte Festplatten) sind so zu vernichten, dass ihre Daten nicht wiederherstellbar sind.

- Datenlöschung und -vernichtung:
  Die Daten auf löschbaren digitalen Informationsträgern sollten so gelöscht werden, dass eine Wiederherstellung praktisch unmöglich ist. Dies kann z. B. durch die folgenden Methoden realisiert werden:
  - Löschsoftware, die nach anerkannten Standards arbeitet,
  - magnetische Entmagnetisierung.

  Elektronische Datenträger wie optische Informationsträger (Datenträger und Akten) sollten auch nach dem Löschen immer durch Schreddern physisch zerstört werden.
- Mobile Endgeräte (Smartphones, Tablets):
  Abhängig vom Gerät, ist eine unterschiedliche Vorgehensweise erforderlich. Ein Zurücksetzen auf die Werkseinstelllungen ist nicht in jedem Fall hinreichend. Deshalb sollte die Datenlöschung immer durch die IT-Abteilung erfolgen.

- Dokumentation der Löschung oder Entsorgung:
  Jede Löschung oder Entsorgung vertraulicher oder streng vertraulicher Informationsträger sollte mittels Lösch- bzw. Entsorgungsprotokoll dokumentiert werden.
- Verantwortlichkeiten:
  Es muss klar festgelegt werden, wer für die Löschung und Entsorgung der Informationsträger verantwortlich ist und wer die Löschprozesse überprüfen oder freigeben muss.

Sofern bei der Vernichtung von Informationsträgern oder der Entsorgung von Informationsträgern, sollte die Einhaltung der Vorgaben aus der Datenschutz-Grundverordnung (DSGVO) und ISO/IEC 21964 (DIN 66399) vertraglich vereinbart werden.

8. Benutzerwechsel digitaler Informationsträger

Erfolgt bei digitalen Informationsträgern ein interner Benutzerwechsel ist dafür zu sorgen, dass Daten des vorherigen Benutzers sicher entfernt sind und der neue Benutzer einen informationstechnisch sauberen und sicheren Informationsträger erhält.

- Löschung und Bereinigung der Daten:
  Vor einer Übergabe digitaler Informationsträger an einen neuen Benutzer sollten alle personenbezogenen, vertraulichen oder sensiblen Daten des vorherigen Benutzers sicher gelöscht werden. Dies kann durch anerkannte Löschverfahren (siehe 7.) erfolgen.
- Rücksetzung auf Werkseinstellungen:
  Falls der Informationsträger ein Gerät mit Betriebssystem (z. B. Laptop/Notebook, Smartphone, Tablet) ist, sollte es auf die Werkseinstellungen zurückgesetzt werden, um jegliche benutzerspezifische Daten und Einstellungen zu entfernen.
- Überprüfung der Zugriffskontrollen und Berechtigungen:
  Die Zugriffsrechte und Berechtigungen des Informationsträgers sollten an die Anforderungen des neuen Benutzers angepasst werden.
  Berechtigungen des vorherigen Nutzers sollten entfernt und neue Rechte entsprechend den Aufgaben und Sicherheitsanforderungen des neuen Benutzers gesetzt werden.
- Änderung der Authentifizierungsdaten:
  Alle benutzerbezogenen Authentifizierungsdaten (z. B. Passwörter, PINs, biometrische Daten) sollten für den neuen Benutzer neu eingerichtet und die alten Daten entfernt werden.
- Dokumentation des Benutzerwechsels:
  Der Wechsel sollte dokumentiert werden, einschließlich der durchgeführten Maßnahmen zur Datenlöschung, der Identität des neuen Benutzers und des Übergabedatums. Diese Dokumentation dient der Nachvollziehbarkeit und Compliance.

9. Schulung und Sensibilisierung

Mitarbeiter, die mit der Verwaltung, Verwendung, Reparatur, Löschung und Entsorgung von Informationsträgern betraut sind, sollten regelmäßig zu Sicherheitsmaßnahmen und den geltenden Richtlinien geschult werden, um sicherzustellen, dass sie potenzielle Risiken kennen und angemessene Sicherheitsmaßnahmen ergreifen.

10. Überwachung und Überprüfung

Die Einhaltung dieser Richtlinie sollte regelmäßig überprüft werden, um festzustellen, ob zusätzliche Schutzmaßnahmen erforderlich sind und ob die hier definierten Maßnahmen noch angemessen sind.

11. Dokumentenlenkung und Änderungshistorie

Diese Richtlinie wird über das Intranet zur Verfügung gestellt.

Dokumentenlenkung

Lenkungskriterien	
Klassifizierung der Wichtigkeit (1-10)	
Klassifizierung der Vertraulichkeit	☐ Öffentlich
	☐ Intern
	☐ Vertraulich
	☐ Streng vertraulich
Speicherort	[z.B. URL der Datei auf dem Server]
Verantwortlicher	
Aktuelle Version	1.0
Datum Erstellung / letzte Änderung	31.10.2025
Nächstes Dokumenten-Review	31.10.2026

Dokumentenhistorie

Version	Freigegeben am	Freigegeben durch	Kommentar
1.0	31.10.2025		

Hinweis zur Nutzung der Vorlage für das Thema

Diese Arbeitshilfe soll nur eine ausführliche Vorlage für eine Richtlinie zum Umgang mit Informationsträgern IT darstellen. Sie wurde nach bestem Wissen und Gewissen recherchiert, zusammengestellt und überprüft. Sie erhebt aber keinen Anspruch auf Vollständigkeit oder Eignung für den Einzelfall und erlaubt keine ausschließliche Anwendbarkeit für ein Unternehmen.

Jede Person, die dieses Produkt erwirbt ist verpflichtet, ihre individuellen Ergänzungen und Anpassungen vorzunehmen und alle Inhalte für den eigenen Anwendungsfall zu prüfen, d.h. diese ggf. mit eigenen Texten zu erweitern oder nicht passende Inhalte zu entfernen.

Die nachfolgende Liste gibt Ihnen einige Hinweise, worauf Sie bei der Ergänzung mit eigenen Texten bzw. Textmodulen unbedingt achten sollten:

1. Wählen Sie einfache, allgemein verständliche Formulierungen und schreiben Sie keine „Bandwurmsätze“.
2. Benutzen Sie eine verständliche Wortwahl und vermeiden Sie Fachvokabular.
3. Formulieren Sie nicht zu sehr ins Detail gehend.
4. Sprechen Sie den Leser in der „Wir“-Form an, um den Zusammenhalt in der Firma zu stärken.
5. Geben Sie den Mitarbeitern im Rahmen von Workshops die Gelegenheit auf die Formulierungen Einfluss zu nehmen.
6. Denken Sie daran, ggf. den Betriebsrat einzubeziehen.
7. Schreiben Sie gendergerecht. Die Nennung aller Geschlechter drückt die Wertschätzung gegenüber allen Menschen aus, unabhängig ihres Geschlechts.

Hinweise zur Anpassung des Dokumentes an die Organisation:

Um das Tool an Ihre Dokumentenstruktur anzupassen, gehen Sie (hier am Beispiel der Version MS Office 2010 dargestellt) bitte folgendermaßen vor:

1. Aktivieren Sie in der Leiste „Start“, Gruppe „Absatz“ das Symbol „Alle anzeigen“. Alternativ können Sie in der Leiste „Datei“ auf „Optionen“ klicken, im sich öffnenden Fenster „Anzeige“ auswählen und das Häkchen bei „alle Formatierungszeichen anzeigen“ setzen.
2. Löschen Sie nun zuerst das Textfeld mit dem Titel und danach die Grafik, indem Sie diese Objekte jeweils markieren und die Entfernen-Taste (Entf) betätigen.
3. Danach löschen Sie den verbliebenen Abschnittswechsel (oben), indem Sie diesen markieren und ebenfalls die Entfernen-Taste (Entf) betätigen.
4. Mittels „Doppelklick“ auf die Kopf- oder Fußzeile können Sie diese nun öffnen und die Texte und deren Formatierungen entsprechend Ihren Wünschen gestalten.
5. Löschen Sie das Kopfzeilen-Logo wie vorher, indem Sie dieses markieren und die Entfernen-Taste (Entf) betätigen.
6. Ein neues Logo fügen Sie ein, indem Sie in der Leiste „Einfügen“, Gruppe „Illustrationen“ auf das Icon „Grafik“ klicken und Ihre Datei auswählen.
7. Diese Hinweisseite entfernen Sie, indem Sie (ab dem letzten Seitenumbruch) alles markieren und die Entfernen-Taste (Entf) betätigen.

Nutzungsbedingungen von Fachinformationen:

(1) Für vorsätzliche oder grob fahrlässige Pflichtverletzungen haftet der Lizenzgeber. Dies gilt auch für Erfüllungsgehilfen.
(2) Für Garantien haftet der Lizenzgeber unbeschränkt.
(3) Für leichte Fahrlässigkeit haftet der Lizenzgeber begrenzt auf den vertragstypischen, vorhersehbaren Schaden.
(4) Der Lizenzgeber haftet nicht für Schäden, mit deren Entstehen im Rahmen des Lizenzvertrags nicht gerechnet werden musste.
(5) Für Datenverlust haftet der Lizenzgeber nur, soweit dieser auch bei der Sorgfaltspflicht entsprechender Datensicherung entstanden wäre.
(6) Eine Haftung für entgangenen Gewinn, für Schäden aus Ansprüchen Dritter gegen den Lizenznehmer sowie für sonstige Folgeschäden ist ausgeschlossen.
(7) Der Lizenzgeber haftet nicht für den wirtschaftlichen Erfolg des Einsatzes der Tools oder Trainings.
(8) Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.

Hinweis auf geschützte Abschnitte bei Nutzung als Formular:

Das Dokument ist abschnittsbezogen als Formular geschützt, sodass Sie z.B. die Kontrollkästen oder Dropdown-Felder (im Sinne eines Formulars) am PC direkt anwählen und ausfüllen können. Es ist kein Kennwort festgelegt.

Schutz entfernen in MS Office 2003:
Symbolleiste „Formular“ aktivieren und auf das „Schloss-Symbol“ klicken.

Schutz entfernen in MS Office 2010:
In der Symbolleiste „Überprüfen“ das Symbol „Bearbeitung einschränken“ aktivieren. Daraufhin öffnet sich das Fenster „Formatierung und Bearbeitung“. In diesem Fenster rechts unten auf die Schaltfläche „Schutz aufheben“ klicken.

Wollen Sie die integrierte Funktionalität nicht nutzen, können Sie die Felder aus der Tabelle einfach entfernen.