B to B - Praxistools für Unternehmen und Freiberufler

knowNOW
TOOLS FOR BUSINESS SUCCESS

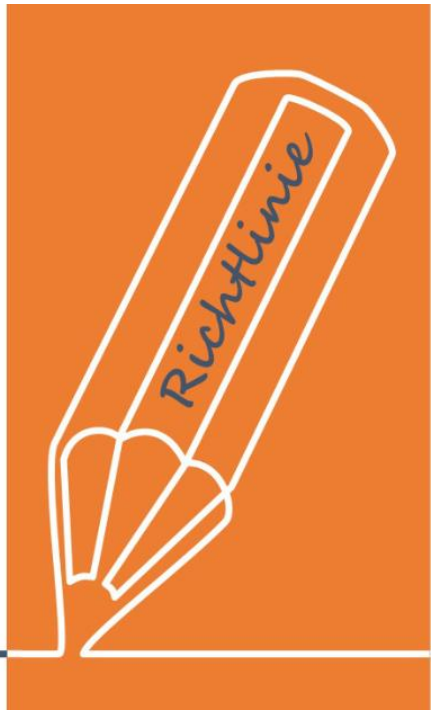
Zentrale Richtlinie Informationssicherheit

UseNOW - TeachNOW - LearnNOW - FindNOW

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

Zentrale Richtlinie Informationssicherheit

des Unternehmens



Ihr Vorteil als Know-NOW User:

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter

www.know-now.de/join

Inhaltsverzeichnis

Sie möchten sich über dieses und weitere Tools informieren?

... nutzen Sie unseren Tool-Online-Shop:

Registrieren und downloaden!

Ihr Vorteil als Know-NOW User:

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter
www.know-now.de/join

1. Zweck und Bedeutung der Informationssicherheit

Die Informationssicherheit und deren Gewährleistung gewinnen mit zunehmender Digitalisierung fortlaufend an Bedeutung.
Auch für unser Unternehmen wird die Absicherung der IT-Systeme gegenüber Ausfällen und der Schutz der IT-Infrastruktur vor unbefugten Zugriffen immer wichtiger, da das Vertrauen interessierter Parteien in unsere Produkte bzw. Leistungen unser wertvollstes Kapital darstellt.
Um dieser Herausforderung adäquat zu begegnen, haben wir diese übergeordnete Richtlinie verfasst, um die Maßnahmen zur Sicherung der Daten unserer Kunden, Partner und Beschäftigten zu koordinieren. Bei dem folgenden Dokument handelt es sich somit um die zentrale Richtlinie zur Informationssicherheit und zum Datenschutz, die den Arbeitsschwerpunkt weiterer diesbezüglicher Richtlinien darstellt.

2. Geltungsbereich

Diese Richtlinie gilt für alle Beschäftigten, Dienstleister und alle anderen relevanten Parteien, die auf die sicherheitsrelevanten Bereiche unserer IT-Systeme und geschützten Informationen bzw. personenbezogenen Daten des Unternehmens zugreifen.

3. Informationssicherheit allgemein

Gemäß unserem Leitbild ist unser Bestreben, uns fortlaufend zu verbessern, um die Zufriedenheit unserer Kunden zu steigern sowie bei allen interessierten Parteien eine hohe Akzeptanz zu erzielen. Um dies zu realisieren, richten wir unsere Zielsetzungen an den Faktoren

- **Vertraulichkeit**
- **Verfügbarkeit und**
- **Integrität von Informationen** aus.

Hierzu- verfolgen wir im Rahmen des Informationssicherheitsmanagements die folgenden übergeordneten Zielsetzungen:

Sie möchten sich über dieses und weitere Tools informieren?
... nutzen Sie unseren Tool-Online-Shop:
Registrieren und downloaden!

- **Sicherstellung der Leistungsfähigkeit**
  Die Sicherstellung der Fähigkeit, unseren Kunden unterbrechungsfrei die vereinbarten Produkte bzw. Dienstleistungen bereitstellen zu können, hat für uns oberste Priorität. Auswirkungen durch technische und organisatorische Maßnahmen unbedingt zu vermeiden und die Verfügbarkeit der IT-Systeme ist entsprechend abzusichern. Für Notfallsituationen haben wir präventiv Notfallpläne ausgearbeitet.
- **Bewusstsein für Informationssicherheit**
  Die Grundlage die Informationssicherheit auf dem erforderlichen Niveau zu gewährleisten ist, dass alle Beschäftigten die potenziellen Gefährdungen kennen und entsprechend verantwortlich handeln. Neben organisatorischen Maßnahmen sorgen wir für regelmäßige Fortbildungen zur Informationssicherheit.
- **Einhaltung von Gesetzen und Vorschriften**
  Unsere Maßnahmen für die Informationssicherheit tragen flankierend auch zur

Einhaltung der für unsere Organisation relevanten Vorschriften, vertraglichen Verpflichtungen und Gesetze bei.

- **Vermeidung finanzieller und materieller Schäden**
  Die unbefugte Veränderung von Daten oder der Verlust der für den Geschäftsbetrieb benötigten Daten und zur Verfügung stehenden IT-Systeme haben in der Regel materielle als auch finanzielle Schäden zur Folge. Diese gilt es zu vermeiden.
- **Schutz von Persönlichkeitsrechten und Betriebsgeheimnissen**
  Vertraulichkeit und Integrität der Daten und Informationen, die in der Organisation verarbeitet werden, sind zu schützen, egal in welcher Form sie vorliegen. Den Anweisungen zum Umgang mit elektronischen Informationen sowie sonstigen Dokumenten in Bezug auf deren Geheimhaltung verpflichten wir uns strikt zu folgen.

Ihr Vorteil als Know-NOW User:

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter

www.know-now.de/join

4. Messbare Informationssicherheitsziele

Von diesen Zielsetzungen leiten wir messbare Sicherheitsziele ab, legen für den Zeitraum eines Jahres Maßnahmen zu deren Erreichung fest und überprüfen den Status im Rahmen der regelmäßigen Managementbewertung. Da wir die Zielsetzungen für jede Periode überprüfen und ggf. anpassen, nutzen wir zur Abbildung des aktuellen Stands das folgende Dokument:

Formular „Zielsetzungen der jährlichen Informationssicherheitsziele“

5. Selbstverpflichtung der obersten Leitung

Die oberste Leitung bekennt sich zu dieser zentralen Richtlinie und damit insgesamt zum Betrieb des Managementsystems zur Gewährleistung der Informationssicherheit. Sie stellt die erforderlichen personellen, organisatorischen und finanziellen Mittel zur Verfügung, um das Informationsmanagementsystem aufrechtzuerhalten und fortlaufend zu verbessern.

Die zentrale Richtlinie zur Informationssicherheit wird von der obersten Leitung freigegeben und organisationsweit veröffentlicht. Mit dieser Richtlinie und deren Aussagen wird der zentrale Aspekt der Informationssicherheit benannt, an den weitere Richtlinien thematisch angelehnt werden.

6. Überprüfung und Sanktionen

Die Einhaltung der Vorgaben des Informationssicherheitssystems werden regelmäßig durch interne Audits im Rahmen eine Auditprogramms überprüft. Anlassbezogene Überprüfungen ergänzen das Auditprogramm.

Verstöße gegen die Vorgaben werden geahndet und ggf. mit arbeitsrechtlichen Maßnahmen geahndet.

Sie möchten sich über dieses und weitere Tools informieren?

... nutzen Sie unseren Tool-Online-Shop:

Registrieren und downloaden!

know NOW

7. Verantwortlichkeiten

Ihr Vorteil als Know-NOW User:

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter

www.know-now.de/join

- **Eigenverantwortung aller Beschäftigten:**
  Verantwortlich für die Umsetzung dieser zentralen Richtlinie sowie den Hinweis auf mögliche bzw. bekannte Schwachstellen und/oder Verbesserungspotenziale.

- **Informationssicherheitsbeauftragte(r):**
  Verantwortlich für die Koordination operativer Tätigkeiten und Maßnahmen zum Betrieb des Managementsystems zur Sicherstellung der IT-Sicherheit sowie der Bewertung von Informationssicherheitsereignissen und Steuerung des Reaktionsprozesses bei Sicherheitsvorfällen.

- **IT-Abteilung, IT-Dienstleister:**
  Zuständig für die operative Planung und Umsetzung aller erforderlichen Aktivitäten bis hin zur Entsorgung von technischem Equipment.

- **Datenschutzbeauftragte(r):**
  Die bzw. der Datenschutzbeauftragte wird von der obersten Leitung benannt und unterstützt alle weiteren Rollen in der Organisation bei der konformen Umsetzung der Verarbeitung personenbezogener Daten.

- **Prozessverantwortliche bzw. Prozessmanager:**
  Die Prozessverantwortlichen sind für die effektive sowie effiziente Umsetzung der Maßnahmen der Informationssicherheit im Rahmen der Leitung und Lenkung ihrer Prozesse verantwortlich. Sie überwachen hierzu die informationssicherheitsrelevanten Kennzahlen und im speziellen die Erreichung der vereinbarten Sicherheitsziele.

  Die Prozessverantwortlichen bzw. Prozessmanager liefern die jeweiligen Eingaben für die Managementbewertung.
  Im Rahmen prozessbezogener Risiken sind sie mit dem Risikoeigentümer gleichzusetzen, da sie für die Behandlung sowie Überwachung dieser Risiken verantwortlich sind. Somit überprüfen sie regelmäßig die Wirksamkeit der Behandlungsmaßnahmen.

- **Asset-Eigentümer:**
  Die Organisation ermittelt und überwacht regelmäßig die materiellen und immateriellen Werte (Assets), die für die Informationssicherheit eine Rolle [illegible] Da die Assets einer Veränderungsdynamik unterliegen, nutzen wir zur Abbildung des aktuellen Stands das folgende Dokument:

  Formular „Asset-Inventar“

Sie möchten sich über dieses und weitere Tools informieren?

... nutzen Sie unseren Tool-Online-Shop:

Registrieren und downloaden!

Ihr Vorteil als Know-NOW User:

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter
www.know-now.de/join

8. Risikomanagement

Die Identifikation und Bewertung von Risiken ist ein zentraler Bestandteil unseres Managementsystems für Informationssicherheit, um unsere Schutzziele zu realisieren. Die Bewertung der Risiken erfolgt systematisch mittels folgender definierter Kriterien:

- Eintrittswahrscheinlichkeit eines Risikos
- Tragweite bzw. potenzieller Schaden, falls das Risiko eingetreten ist.

Informationssicherheitsrisiken werden durch den Risikoeigentümer dokumentiert, bei Bedarf behandelt und fortgeschrieben. Die detaillierte Vorgehensweise ist in einem dezidierten Dokument beschrieben.

9. Informationssicherheitsereignisse und Vorfälle

Ist ein Ereignis in der Organisation wahrscheinlich sicherheitsrelevant, wird es als Informationssicherheitsereignis eingestuft und muss gemeldet werden. In einem weiteren Dokument ist die vorgeschriebene für wesentliche Schritte der Behandlung von Informationssicherheitsereignissen und Vorfällen z.B. für die folgenden Aspekte geregelt:

- Kommunikation von Ereignissen und Vorfällen
- Untersuchung und Klassifizierung von Vorfällen
- Reaktion auf Ereignisse oder Vorfälle
- Verlust von Geräten und Datenträgern im Unternehmenseigentum
- Dokumentation und Nachbereitung von Vorfällen
- Überprüfung, Sensibilisierung und Verbesserung

Beschäftigte sind nicht befugt, nach eigenem Ermessen Information im Zusammenhang mit Informationssicherheitsereignissen und Vorfällen nach außen zu tragen.

10. Informationssicherheitsbewusstsein und Schulungen

Die Organisation bietet den Beschäftigten im Rahmen ihres Personalmanagements regelmäßige Grundlagenschulungen zum Thema Informationssicherheit an, um das Bewusstsein zu schärfen und die fachliche Handlungskompetenz zur Erfüllung der in den Richtlinien formulierten Anforderungen zu schaffen. Ein zielgruppenorientiertes Schulungskonzept sensibilisiert für die Risiken beim Umgang mit Informationen.

Weiterhin werden die folgenden Maßnahmen ergriffen:

- Vertragliche Verpflichtung aller Beschäftigten zur Einhaltung der Informationssicherheit.
- Vertragliche Regelungen mit externen Dienstleistern und Kooperationspartnern.
- Ausrichtung der Organisation an IT-relevanten regulatorischen und vertraglichen Bestimmungen.

Sie möchten sich über dieses und weitere Tools informieren?
... nutzen Sie unseren Tool-Online-Shop:
Registrieren und downloaden!

Ihr Vorteil als Know-NOW User:

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter www.know-now.de/join

11. Themenspezifische Sicherheitsrichtlinien

Diese zentrale Richtlinie für die Informationssicherheit wird durch weitere themenspezifische Sicherheitsrichtlinien, -verfahren und Formblätter ergänzt und unterstützt. Die Erstellung dieser zusätzlichen Richtlinien und Dokumente erfolgt durch die jeweilig fachlich kompetente Stelle. Die Befugnis für deren Freigabe liegt bei der/den Informationssicherheitsbeauftragten.

Alle Beschäftigten müssen diese Richtlinien anwenden und einhalten, soweit diese für ihre Position bzw. Rolle und Organisationseinheit gelten.

Für die folgenden Themenbereiche ist unter anderem vorgesehen, ergänzende sicherheitsrelevante Richtlinien und Verfahren zu erstellen:

- Informationssicherheitsprozesse im Projektmanagement
- Sicherheitsanforderungen an Cloud-Dienste
- Informationsklassifizierung
- Risikomanagement IT
- Informationssicherheitsvorfälle IT
- Notfallbetriebsverfahren (BCP = Business Continuity Plan)
- Mobiles Arbeiten
- Umgang mit Informationsträgern (Entsorgung)
- Kryptografie
- Nutzerauthentifizierung
- Benutzerzugänge zu IT-Systemen (Kennwörter)
- Zugriffsmanagement
- Änderungsmanagement IT
- Entwicklung von Software
- Schutz vor Schadsoftware
- Patch-Management
- Netzwerkplanung und Netzwerksicherheit
- Datensicherung
- Beschaffung von IT-Leistungen (Vergabe von Unteraufträgen durch den IT-Dienstleister)
- Netzwerksicherheit
- IT-Cloud-Anbieterverzeichnis mit Regelungen zur Rückgabe und Mandantentrennung
- Verarbeitung personenbezogener Daten

Diese können als einzelnes ggf. neues Dokument erstellt und gelenkt, werden oder es kann eine thematische Zusammenfassung und Lenkung, ggf. mit bereits vorhandenen Dokumenten, erfolgen.

Sie möchten sich über dieses und weitere Tools informieren?

... nutzen Sie unseren Tool-Online-Shop:

Registrieren und downloaden!

Ihr Vorteil als Know-NOW User:

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter

www.know-now.de/join

12. Kundenvorgaben an die Informationssicherheit

Die nachfolgende Auflistung enthält Dokumente auf die sich unsere Kunden in Verträgen beziehen und die somit durch uns zu erfüllende Anforderungen an die Informationssicherheit festlegen. Dies können zum Beispiel gesetzliche oder behördliche Vorgabedokumente sowie auch Normen oder Branchenstandards sein:

- *Dokument 1*
- *Dokument 2*

13. 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	15.07.2025
Nächstes Dokumenten-Review	15.07.2026

Dokumentenhistorie

Version	Freigegeben am	Freigegeben durch	Kommentar
1.0	15.07.2025		

Sie möchten sich über dieses und weitere Tools informieren?

... nutzen Sie unseren Tool-Online-Shop:

Registrieren und downloaden!

Hinweise der Zuordnung zur DIN EN ISO 27001 bzw. TISAX®

VDA® ISA-Kontrollfrage 1.1.1, Ziel:
„Die Organisation benötigt mindestens eine Richtlinie für Informationssicherheit. Diese spiegelt die Wichtigkeit und Bedeutung der Informationssicherheit wider und ist an die Organisation angepasst. Zusätzliche Richtlinien können je nach Größe und Aufbau der Organisation sinnvoll sein.“

DIN EN ISO 27001, Anhang A 5.1, Informationssicherheitspolitik und -richtlinien:
„Informationssicherheitspolitik und themenspezifische Richtlinien müssen definiert, von der Geschäftsleitung genehmigt, veröffentlicht, dem zuständigen Personal und den interessierten Parteien mitgeteilt und von diesen zur Kenntnis genommen sowie in geplanten Abständen und bei wesentlichen Änderungen überprüft werden.“

Hinweise zur Nutzung der Vorlage

Diese Arbeitshilfe soll nur eine ausführliche Vorlage für eine „Zentrale Richtlinie Informationssicherheit“ 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 erklären Sie nicht vermeidbares Fachvokabular.
3. Formulieren Sie nicht zu sehr ins Detail gehend.
4. Geben Sie den Mitarbeitern im Rahmen von Workshops die Gelegenheit auf die Formulierungen Einfluss zu nehmen.

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.