

# Kostenlose Vorlage: Richtlinie zur Informationssicherheit

Bei diesem Dokument handelt es sich um eine kostenlose Vorlage bzw. Checkliste der activeMind AG zu den Themenbereichen Datenschutz und Datensicherheit. Die aktuellste Version finden Sie stets auf [im Downloadbereich unserer Website](https://www.activemind.de/datenschutz/dokumente/).

Sie können dieses Dokument an die Bedürfnisse in Ihrem Unternehmen anpassen, speichern und ausdrucken. Bitte haben Sie Verständnis dafür, dass die activeMind AG keinerlei Haftung für etwaige Fehler übernimmt.

Bei Fragen oder Problemen helfen wir Ihnen gerne weiter!

Ihr Team der activeMind AG

Telefon: +49 (0)89 / 91 92 94 - 900  
E-Mail: [anfrage@activemind.de](mailto:anfrage@activemind.de)  
Web: <https://www.activemind.de>

# Richtlinie zur Informationssicherheit

Die Leitlinie zur Informationssicherheit ist ein wichtiges Grundsatzdokument der Geschäftsführung zur Geschäftsstrategie, den verbindlichen Prinzipien und dem anzustrebenden Niveau der Informationssicherheit im Unternehmen. Damit das Unternehmen dieser Verantwortung nachkommen kann, müssen sämtliche Mitarbeiter den Schutz der Informationstechnik unterstützen. Die Entwicklung der Leitlinie muss von der Geschäftsführung angestoßen und aktiv begleitet werden.

Der Informationssicherheitsbeauftragte (ISB) sollte die Leitlinie in enger Kooperation mit der Geschäftsführung erarbeiten und dabei von weiteren Verantwortlichen für Informationssicherheit unterstützt werden. Die Leitlinie zur Informationssicherheit muss allen Mitarbeitern bekannt gegeben und kontinuierlich aktualisiert werden.

Die Leitlinie sollte folgende Punkte beinhalten:

## Präambel

Fügen Sie hier eine Kurzbeschreibung Ihres Unternehmens und die Motivation zur Einhaltung der Informationssicherheit in Ihrem Unternehmen ein. Sollen mit dieser Leitlinie besondere Ziele erreicht werden, gehören diese Informationen auch hierher.

## Geltungsbereich

Beschreiben Sie hier den Geltungsbereich. Dieser bestimmt den Anwendungsbereich (Scope) für die gesamte Organisation und begründet dies.

## Informationssicherheitsziele

Beschreiben Sie hier die Sicherheitsziele des Unternehmens. Bestimmen Sie diese sorgfältig, damit Sicherheitsstrategien und -konzepte erarbeitet werden können, welche die Anforderungen des Unternehmens erfüllen. Diese Informationen bilden einen guten Ausgangspunkt für eine Risikoanalyse und -bewertung.

Das oberste Ziel sollte sein die Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit der eigenen und der von Kunden und Geschäftspartnern anvertrauten Informationen und Ressourcen zu schützen. Zusätzlich müssen gesetzliche und vertragliche Anforderungen stets eingehalten werden.

Beschreiben Sie hier im Detail die obersten Ziele bzgl.:

* Vertraulichkeit
* Vertraulichkeit
* Integrität
* Authentizität
* Verbindlichkeit
* Compliance

Neben diesen Zielen gibt es eine Reihe spezieller Ziele, die durch den Aufbau, die Ausrichtung und das Selbstverständnis des Unternehmens bedingt sind, z.B. die stetige und messbare Verbesserung des gesamten Informationssicherheits-Managementsystems (ISMS). Diese Ziele sollten hier beschrieben werden.

Aus den grundsätzlichen Zielen des Unternehmens und den allgemeinen Rahmenbedingungen sollten dann allgemeine Sicherheitsziele abgeleitet werden. Auf Basis dieser Detailziele kann auf nachgeordneter/tieferer Ebene die Informationssicherheitsleitlinie durch themenspezifische Richtlinien unterstützt werden, welche zusätzlich die Umsetzung von Maßnahmen zur Informationssicherheit anordnen. Diese weiteren Richtlinien sollten so aufgebaut sein, dass die Bedürfnisse gewisser Zielgruppen im Unternehmen angesprochen oder bestimmte Themen abgedeckt werden.

## Bedeutung der Sicherheit

Beschreiben Sie hier, warum Informationssicherheit ein integraler Bestandteil Ihrer Unternehmenskultur ist.

## Organisation

Schaffen Sie zur Erfüllung und Überwachung sämtlicher Daten- und Informationssicherheitsvorgaben in Ihrem Unternehmen eine geeignete Sicherheitsorganisation und benennen Sie Verantwortliche. Legen Sie Rollen fest und ordnen Sie diesen die entsprechenden Aufgaben zu. Diese Rollen müssen dann qualifizierten Mitarbeitern übertragen und von diesen ausgeführt werden.

Folgende Rollen sollten mindestens definiert werden:

* Gesamtverantwortung (obliegt grundsätzlich der Geschäftsführung)
* Informations- bzw. IT-Sicherheitsbeauftragter
* Ggf. Datenschutzbeauftragter
* Mitarbeiter

## Schulung und Sensibilisierung

Alle Mitarbeiter müssen in Hinblick auf die Bedeutung von Sicherheitsmaßnahmen und ihre Anwendung geschult und sensibilisiert werden. Beschreiben Sie hier Sicherheitsschulungen und Sensibilisierungsmaßnahmen.

## Regelwerke

Die Sicherheitsleitlinie sollte durch themenspezifische Richtlinien unterstützt werden, die zusätzlich die Umsetzung von Maßnahmen zur Informationssicherheit anordnen. Konkretisieren Sie hier die Anforderungen an diese untergeordneten Richtlinien und definieren Sie die Hierarchie der Dokumente. Zusätzlich müssen Maßnahmen zur Überprüfung dieser Regelwerke festgelegt werden.

## Informationssicherheitsvorfälle

Beschreiben Sie hier den Umgang mit Informationssicherheitsvorfällen und gehen Sie insbesondere auf Meldewege, Umgang, Verbesserung und Dokumentation von Informationssicherheitsereignissen und Schwachstellen ein.

## Einhaltung von Vorgaben

Beschreiben Sie hier, welche gesetzliche Vorgaben für das Unternehmen relevant sind und wie diese eingehalten werden.

## Prüfung und Überwachung

Das erreichte Sicherheitsniveau der Organisation, Prozesse und Systeme sollten durch eine Kombination aus periodisch wiederkehrenden Prüfungen und kontinuierlichen Kontrollen überwacht werden. Beschreiben Sie diesbezüglich die Vorgehensweise in Ihrem Unternehmen.

## Verstöße und Folgen

Klären Sie hier die Mitarbeiter darüber auf, welche Sanktionen bei Zuwiderhandlungen drohen.