

Leitlinie zur Informationssicherheit

# managedhosting.de

Leitlinie zur Informationssicherheit



# Leitlinie zur Informationssicherheit

## Inhaltsverzeichnis

Leitlinie zur Informationssicherheit.....	2
Allgemeine Dokumentinformationen.....	2
Status.....	2
Formale Angaben.....	2
Präambel.....	2
Definition.....	3
Anwendungsbereich.....	3
Stellenwert im Unternehmen.....	4
Zielsetzung.....	4
Sicherheitsniveau.....	4
Verantwortlichkeiten.....	5
Prozess zur Umsetzung.....	5
Strategie, Maßnahmen und deren Umsetzung.....	5
Besondere Maßnahmen für Cloud-Services.....	5

## Allgemeine Dokumentinformationen

### Status

**Verantwortlicher:** Roberto Schulz

**Stand:** 24.09.2024

**Version:** 11

**Vertraulichkeitsstufe:** Öffentlich

**Status:** veröffentlicht

**Nächster Review Termin:** 01.07.2025

**Inkrafttreten:** 01.07.2013

**Gültigkeit:** Dieses Dokument ist gültig, bis es durch eine aktualisierte Version ersetzt wird.

### Formale Angaben

**Aufbewahrungsort:** FileCloud\Team Folders\compliance\ISMS\Leit- und Richtlinien

**Dokument:** ISO27001 - MH - 01-11 - Leitlinie zur Informationssicherheit.odt

**Format:** OASIS Open Document und PDF

**Kommunikation:** Zur verbindlichen Kenntnisnahme für alle Mitarbeiter - Veröffentlichung im Wiki

## Präambel

Gegenstand des Unternehmens ist die Bereitstellung von Cloud-Services in eigenen Rechenzentren zur Erbringung von Informations- und Kommunikationsdienstleistungen (Managed Hosting), die Datenbe- und -verarbeitung einschließlich Datenbanken und Herstellung von Datenverarbeitungsprogrammen, der Handel mit Hard- und Software und allen sonstigen Dienstleistungen, die den vorgenannten Tätigkeiten dienlich sind.

Bedingt durch den Geschäftsgegenstand des Unternehmens ist die managedhosting.de GmbH bei der Erbringung Ihrer Dienstleistungen für gewerbliche Kunden in entscheidendem Maße auf die korrekte Funktion und die Verfügbarkeit der von Ihr betriebenen Cloud-Services angewiesen. Somit hat die ständige Gewährleistung der Informationssicherheit einen sehr hohen unternehmerischen Stellenwert.

Aus diesem Grund hat die Geschäftsführung der managedhosting.de GmbH, in Zusammenarbeit mit deren Informationssicherheitsbeauftragten einen Informationssicherheitsprozess für den Umgang mit den angebotenen Cloud-Services eingeführt. Die Leitlinie zur Informationssicherheit soll deshalb für alle Mitarbeiter und Kunden Aufforderung und Verpflichtung zu verantwortungsbewusstem und gesetzeskonformen Umgang mit der IT-Infrastruktur der managedhosting.de GmbH sein.

Die managedhosting.de GmbH schützt durch die Sicherung ihrer Arbeitsfähigkeit der von ihr betriebenen IT-Infrastruktur ihr Ansehen und ihre unternehmerischen Interessen in der Öffentlichkeit sowie ihre Vertrauenswürdigkeit für Auftraggeber und Partner.

Die Gewährleistung der allgemeinen Informationssicherheitsziele Verfügbarkeit, Vertraulichkeit, Integrität und als erweitertes Schutzziel der Authentizität von Informationen ist deshalb wichtiger Bestandteil der Unternehmensphilosophie der managedhosting.de GmbH. Der Informationssicherheitsprozess ist Gegenstand eines eigenen Informationssicherheitsmanagementsystems (ISMS) nach der Norm ISO 27001 unter besonderer Berücksichtigung der ISO 27017.

Das Management und die Mitarbeiter verpflichten sich auf die Einhaltung und Umsetzung der Ziele und Maßnahmen.

## Definition

Unter **Informationssicherheit** ist der Schutz der von der managedhosting.de GmbH für gewerbliche Kunden betriebenen IT-Infrastruktur vor Störung, Missbrauch und Manipulation zu verstehen.

Ein Ausfall der IT soll insgesamt kurzfristig kompensiert werden können, wobei der Geschäftsablauf durch Sicherheitsmängel nicht stark beeinträchtigt werden darf. Alle Sicherheitsmaßnahmen werden so ausgewählt, dass sie geeignet und angemessen sind. Sie sollten also einerseits das Risiko bestmöglich minimieren und andererseits in geeignetem Verhältnis zu im Schadensfall entstehenden Kosten stehen.

Die Daten unserer Kunden sowie die für unsere Kunden betriebenen IT-Systeme werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandszeiten im Rahmen des vom Kunden beauftragten SLA toleriert werden können.

## Anwendungsbereich

Das ISMS umfasst alle Standorte, Mitarbeiter und Prozesse zur Erfüllung des Geschäftsgegenstands (Managed Hosting und Cloud Services).

Für die Erbringung unserer Dienstleistungen wurden Flächen in unterschiedlichen ausgewählten Datacentern angemietet, die die Tier III-Anforderungen erfüllen. Das beinhaltet die Stellflächen, elektrischen Strom, Klimatisierung und Maßnahmen der physischen Sicherheit. Die Internetanbindung der Standorte erfolgt über mehrere, unabhängig vom Datacenter angemietete IP-Transits. Alle weitere notwendige Technologie gehört zum Anwendungsbereich des ISMS.

Die Abgrenzung des ISMS zu unseren Kunden und Lieferanten ist abhängig von der Ausprägung der Dienstleistung wie in der folgenden Übersicht dargestellt:

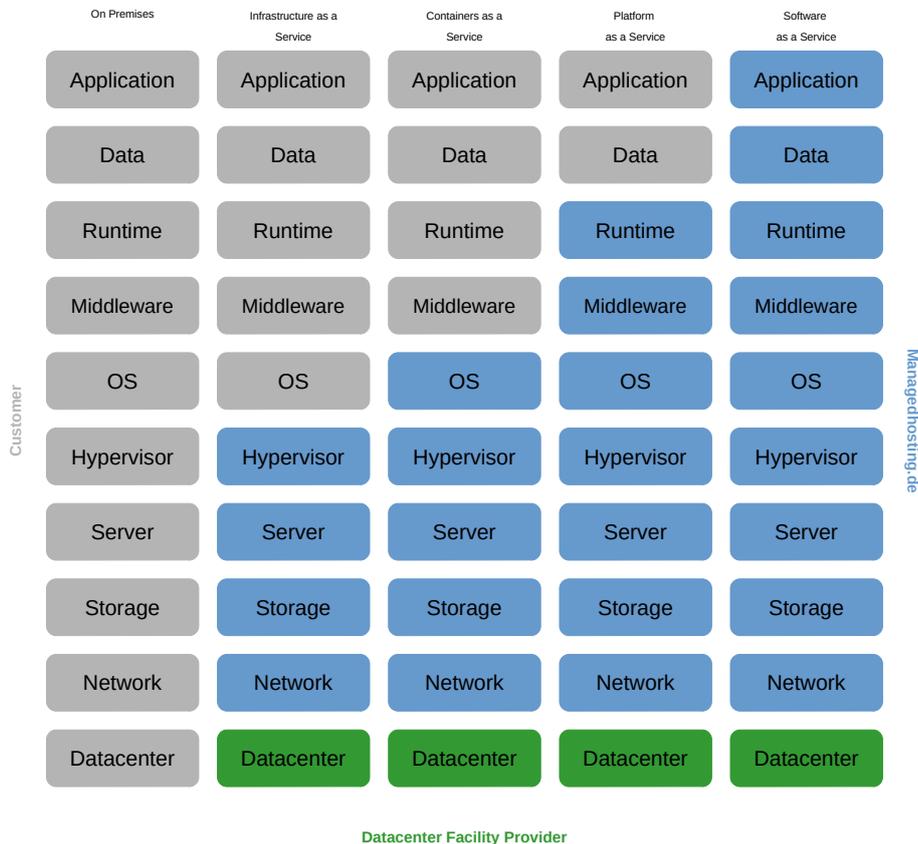


Abbildung 1: Aufteilung der Verantwortlichkeiten für die Technologieebenen zwischen managedhosting.de, Kunden und externem Datacenter Facility Provider



## Stellenwert im Unternehmen

Die Informationssicherheit hat - bedingt durch den Geschäftsgegenstand des Unternehmens - einen sehr hohen unternehmerischen Stellenwert. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel. An die Sicherstellung der Vertraulichkeit von Firmendaten stellen wir die höchsten Ansprüche.

Aus diesem Grund hat die Geschäftsführung der managedhosting.de GmbH, in Zusammenarbeit mit dem Informationssicherheitsbeauftragten der managedhosting.de GmbH einen Informationssicherheitsprozess für den Umgang mit den IT-Einrichtungen eingeführt.

Die Leitlinie zur Informationssicherheit soll deshalb für alle Mitarbeiter, Dienstleister und Kunden Aufforderung und Verpflichtung zu verantwortungsbewusstem und gesetzeskonformen Umgang mit der IT- Infrastruktur der managedhosting.de GmbH sein.

## Zielsetzung

Die managedhosting.de GmbH schützt durch die Sicherung ihrer Arbeitsfähigkeit der von ihr betriebenen IT- Infrastruktur ihr Ansehen und ihre unternehmerischen Interessen in der Öffentlichkeit sowie ihre Vertrauenswürdigkeit für Auftraggeber und Partner.

Die Gewährleistung der allgemeinen Informationssicherheitsanforderungen Verfügbarkeit, Vertraulichkeit, Integrität und als erweitertes Schutzziel der Authentizität von Informationen ist deshalb wichtiger Bestandteil der Unternehmensphilosophie der managedhosting.de GmbH.

Folgende Ziele sollen durch die konsequente und kontinuierliche Umsetzung der Leitlinie zur Informationssicherheit erreicht werden:

- Die managedhosting.de GmbH gewährleistet die Verfügbarkeit der zur Erbringung ihrer Dienstleistungen notwendigen IT- Infrastruktur und unterstützt damit die Kontinuität der Arbeitsabläufe ihrer Kunden.
- IT- Dienstleistungen für Kunden der managedhosting.de GmbH sollen im Rahmen der jeweiligen vertraglichen Vereinbarungen und des durch den Kunden gewählten SLA stets in der geforderten Qualität und ohne Beeinträchtigungen durch Störungen erbracht werden. Daten werden - soweit möglich und mit dem Kunden vertraglich vereinbart - vor Verlust geschützt.
- Die managedhosting.de GmbH stellt den Schutz von Daten und Arbeitsergebnissen vor unberechtigter Kenntnisnahme sicher. Besonders schützenswerte Daten (personenbezogene Daten, Betriebsgeheimnisse) werden im Rahmen einer gesonderten Vereinbarung mit dem Kunden behandelt.
- Die managedhosting.de GmbH schützt die zur Erbringung ihrer Dienstleistungen notwendigen IT- Infrastruktur und Daten vor Verfälschung bzw. unberechtigter Veränderung
- Die managedhosting.de GmbH schützt die zur Erbringung ihrer Dienstleistungen notwendigen IT- Infrastruktur und Daten vor Manipulation und Missbrauch, d.h. vor zweckwidriger Nutzung oder Nutzung durch Unbefugte.
- Die managedhosting.de GmbH schützt ihr IT-Netzwerk nach dem Stand Technik gegen unbefugten Zugriff.
- Die managedhosting.de GmbH und ihre Mitarbeiter halten die einschlägigen Gesetze und sonstigen rechtlichen Bestimmungen zum Betrieb von IT-Infrastruktur ein.
- Die managedhosting.de GmbH wahrt die Persönlichkeitsrechte ihrer Mitarbeiter

## Sicherheitsniveau

Diese Leitlinie zur Informationssicherheit bezieht sich auf für gewerbliche Kunden der managedhosting.de GmbH betriebene IT-Infrastruktur mit normalem Schutzbedarf. Ein normaler Schutzbedarf ist gegeben, wenn durch den Verlust an Vertraulichkeit, Integrität und Verfügbarkeit der betroffenen Komponenten

- nur ein geringfügiger Verstoß gegen Vorschriften und Gesetze möglich ist,
- eine Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen nicht möglich ist oder für diesen tolerabel bleibt,
- eine Beeinträchtigung der persönlichen Unversehrtheit des Einzelnen nicht möglich ist,
- die Aufgabenerfüllung der betroffenen Komponente nur geringfügig beeinträchtigt ist,
- nur eine geringe Ansehens- und Vertrauensbeeinträchtigung zu befürchten ist und
- der finanzielle Schaden im Rahmen der normalen Geschäftstätigkeit unerheblich bleibt.

Diese Richtlinien stellen für Komponenten der IT-Infrastruktur mit hohem oder sehr hohem Schutzbedarf eine Grundsicherung dar, reichen aber möglicherweise nicht alleine zur Sicherung aus. Hier müssen ergänzende Maßnahmen auf Basis einer differenzierten Sicherheitsanalyse ergriffen werden.



## Verantwortlichkeiten

Die Verantwortung für die Umsetzung und Einhaltung der Leitlinie zur Informationssicherheit liegt bei der Geschäftsführung der managedhosting.de GmbH. Die Geschäftsführung überträgt die Umsetzung der Leitlinie zur Informationssicherheit und die Kontrolle über deren Einhaltung an den Informationssicherheitsbeauftragten der managedhosting.de GmbH. Die Einhaltung der Informationssicherheitsmaßnahmen durch Mitarbeiter wird im Rahmen des Disziplinarprozesses kontrolliert.

Der Informationssicherheitsbeauftragte der managedhosting.de GmbH nimmt seine Aufgaben in enger Zusammenarbeit mit dem Datenschutzbeauftragten wahr.

Die Geschäftsleitung der managedhosting.de GmbH kann Mitglieder der Geschäftsleitung selbst, Mitarbeiter des Unternehmens oder externe Dienstleister zum Informationssicherheitsbeauftragten sowie Datenschutzbeauftragten bestimmen.

## Prozess zur Umsetzung

Die Umsetzung der Leitlinie zur Informationssicherheit in einen im Unternehmen laufend angewendeten Informationssicherheitsprozess ist Gegenstand eines eigenen Informationssicherheitsmanagementsystems. Dieses ISMS orientiert sich an der Norm ISO 27001. Prozessverantwortlich ist die Geschäftsführung der managedhosting.de GmbH. Sie fördert auch die kontinuierliche Verbesserung des ISMS.

## Strategie, Maßnahmen und deren Umsetzung

Zur Gewährleistung der Umsetzung und Einhaltung der Leitlinie zur Informationssicherheit im Sinne der genannten Ziele werden folgende Maßnahmen in der managedhosting.de GmbH umgesetzt:

- Bereitstellung der technischen und personellen Ressourcen zur Umsetzung der beschlossenen Maßnahmen
- Betreuung der Kunden der managedhosting.de GmbH im Umgang mit der für sie bereitgestellten IT-Infrastruktur bezüglich sicherheitsrelevanter Aspekte
- Abstimmung zwischen Mitarbeitern und Informationssicherheitsbeauftragten über Sicherheitsaspekte neuer Kundenprojekte
- Berücksichtigung der Informationssicherheitsanforderungen in der Zusammenarbeit mit Partnern und externen Dienstleistern
- Festlegung von Konsequenzen bei Verstößen gegen Informationssicherheitsregelungen durch Mitarbeiter
- Planung und Überwachung der Realisierung von Informationssicherheitsmaßnahmen im technischen, organisatorischen, personellen und infrastrukturellen Bereich durch den Informationssicherheitsbeauftragten der managedhosting.de GmbH
- Verabschiedung notwendiger Richtlinien als flankierende Maßnahme zum Informationssicherheitsprozess
- Regelmäßige Schulung der Mitarbeiter in Informationssicherheit

## Besondere Maßnahmen für Cloud-Services

Zur besonderen Absicherung der angebotenen Cloud-Dienstleistungen und zur Erhöhung der Cybersecurity werden folgende Maßnahmen bei Planung und Betrieb der Cloud-Services beachtet:

- Bei der Vergabe von Berechtigungen und der Überwachung von IT-Einrichtungen werden Risiken durch Insider mit besonderen Berechtigungen berücksichtigt.
- Die technischen Möglichkeiten der eingesetzten IT-Systeme zur Mandantentrennung und Isolation der Cloud-Dienstleistungskunden voneinander werden konsequent umgesetzt. Bei der Auswahl von IT-Systemen ist die Mandantenfähigkeit eine notwendige Voraussetzung.
- Der Zugang zu den Werten des Cloud-Dienstleistungskunden durch Mitarbeiter der managedhosting.de GmbH wird erfolgt nur zu den mit dem Kunden vereinbarten Zwecken.
- Die Absicherung der Zugriffsmöglichkeiten auf die Cloud-Dienste, entspricht dem Stand der Technik. Zugriffsrechte werden nur nach bestimmten Prozessen vergeben.
- Notwendige Änderungen werden entsprechend dem vereinbarten SLA angekündigt. Vom Kunden initiierte Änderungen erfolgen nur in Absprache mit dem Kunden.
- Für die Gewährleistung der Sicherheit der Virtualisierung werden die jeweils aktuellen Referenzarchitekturen eines der führenden Anbieter für Virtualisierungstechnologien – VMware – umgesetzt und regelmäßig vom Hersteller zertifiziert.
- Cloud-Kundendaten werden nach dem Stand der Technik gegen den unbefugten Zugriff Dritter geschützt.
- Nach der Übermittlung der Zugangsdaten erfolgt eine Unterstützung des Lebenszyklusmanagement der Konten des Cloud-Dienstleistungskunden nach individueller Absprache.
- Bei Bekanntwerden eines Bruchs der Vertraulichkeit von Daten oder Systemen des Cloud-Dienstleistungskunden wird der Kunde umgehend darüber informiert. Bei Bedarf werden definierte Maßnahmen zur Unterstützung bei der forensischen Analyse angewendet.