Richtlinie - Informationssicherheitsleitlinie

Dokumentenlenkung

Dokumententyp	Richtlinie
Titel	Richtlinie - Informationssicherheitsleitlinie
Eigentümer	Informationssicherheitsbeauftragter
Ersteller	Lars Neumann
Prüfer	Anna Haußmann
Genehmiger	Klaus Burkart
Freigegeben am	26.03.2026
Nächste Aktualisierung	01.12.2026
Version	1.4
Status	freigegeben
Vertraulichkeitsstufe	öffentlich
Prüfungsintervall	jährlich
Empfängerkreis	Vorstand, alle Mitarbeitende und interessierte Externe

Die in diesem Dokument enthaltenen Inhalte finden neben der hsag Heidelberger Service AG uneingeschränkt auch auf die Tochtergesellschaft hsag ON AG Anwendung.

Sämtliche Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter (m/w/x). Die verkürzte Sprachform hat lediglich redaktionelle Gründe und beinhaltet keine Wertung.

Versionshistorie

Version	Datum	Autor	Art der Änderung
0.1	14.04.2025	Nandini Suresh (secjur GmbH)	Erstellung Vorlage
1.0	24.09.2025	Malte Cohrs	Anpassungen Inhalt
1.1	04.11.2025	Malte Cohrs	Anpassungen Inhalt
1.2	21.01.2026	Malte Cohrs	Anpassungen Inhalt
1.3	17.03.2026	Anna Haußmann	Anpassungen Inhalt, Layout
1.4	26.03.2026	Anna Haußmann	Anpassungen Inhalt, Layout

Inhaltsverzeichnis

1. Zweck, Anwendungsbereich und Anwender

Dieses Dokument definiert die Informationssicherheitsleitlinie der Organisation und somit das übergeordnete Ziel des Informationssicherheitsmanagementssystems (ISMS). In diesem Dokument wird der Zweck, die Ausrichtung, die Grundlagen sowie die allgemeinen Regelungen für das ISMS festgelegt.

Die in diesem Dokument festgelegte Informationssicherheitsleitlinie bezieht sich auf das gesamte ISMS gemäß dem definierten Anwendungsbereich.

Die Anwender des Dokuments sind alle Mitarbeitende der Organisation sowie externe interessierte Parteien.

2. Begriffe der Informationssicherheit

Begriff	**Bedeutung**
Vertraulichkeit	die Eigenschaft, dass Informationen nicht unbefugten Personen, Einrichtungen oder Prozessen zugänglich gemacht oder offengelegt werden
Integrität	die Eigenschaft der Richtigkeit und Vollständigkeit der Informationen
Verfügbarkeit	die Eigenschaft, dass Informationen bei Bedarf von einer autorisierten Stelle zugänglich und nutzbar sind
Informationssicherheit	Erhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen
ISMS	Managementprozess, der sich mit Planung, Implementierung, Instandhaltung, Überprüfung und Verbesserung der Informationssicherheit befasst

3. Stellenwert der Informationssicherheit

3.1 Unternehmensziele

Die übergeordneten Unternehmensziele unserer Organisation bilden die strategische Grundlage für den Aufbau und die Weiterentwicklung unseres Informationssicherheits-Managementsystems (ISMS). Ziel ist es, die Initiativen im Bereich der Informationssicherheit konsequent an unserer Vision, Mission und den unternehmerischen Kernzielen auszurichten.

Dabei verfolgen wir insbesondere folgende geschäftliche Zielsetzungen:

- **Sicherung der Geschäftskontinuität:** Schutz kritischer Informationen und Systeme vor Ausfällen, Angriffen oder Datenverlusten zur Gewährleistung eines stabilen Geschäftsbetriebs.
- **Unterstützung der Marktexpansion:** Aufbau eines vertrauenswürdigen Sicherheitsniveaus, das neue Märkte, Partner und Kunden überzeugt und den Eintritt in neue Regionen erleichtert.
- **Förderung von Innovation:** Schutz von geistigem Eigentum und Forschungsdaten, um innovative Produkte und Dienstleistungen sicher entwickeln und vermarkten zu können.

- **Steigerung der Kundenzufriedenheit:** Verlässlicher Umgang mit sensiblen Kundendaten zur Schaffung und Erhaltung von Vertrauen sowie zur Stärkung der Kundenbindung.
- **Rechtssicherheit und Compliance:** Einhaltung gesetzlicher, regulatorischer und vertraglicher Anforderungen zur Minimierung rechtlicher Risiken und Wahrung des guten Rufes des Unternehmens.

Unsere Informationssicherheitsstrategie wird regelmäßig im Kontext unserer strategischen Planung überprüft und angepasst, um sicherzustellen, dass sie die sich ändernden geschäftlichen Anforderungen und externen Rahmenbedingungen aktiv unterstützt.

3.2 Relevante Anforderungen und interessierte Parteien

Insbesondere ist für uns wichtig, dass wir folgende Anforderungen erfüllen:

- Kundenanforderungen
- Vertragliche Anforderungen
- Rechtliche Anforderungen

Die Erfordernisse und Erwartungen folgender interessierten Parteien möchten wir primär mit dem ISMS erfüllen:

- Kunden
- Mitarbeitende
- Vorstand

3.3 Informationssicherheit

Die Informationssicherheit ist ein zentraler Bestandteil unserer Unternehmensstrategie und ein entscheidender Faktor zur Erreichung unserer Unternehmensziele. Die Ziele für das ISMS leiten sich aus der gemäß Kapitel 3.1 beschriebenen Geschäftsstrategie der Organisation sowie gemäß Kapitel 3.2 beschriebenen relevanten Anforderungen und interessierten Parteien ab. Unser Informationssicherheits-Managementsystem (ISMS) basiert auf den drei fundamentalen Prinzipien der Informationssicherheit:

- **Vertraulichkeit**: Schutz sensibler Informationen vor unbefugtem Zugriff, um Kundenvertrauen zu erhalten, Innovationen zu sichern und rechtliche Anforderungen zu erfüllen.
- **Integrität**: Sicherstellung der Korrektheit und Vollständigkeit von Informationen und Systemen, um fundierte Geschäftsentscheidungen treffen und effiziente Prozesse gewährleisten zu können.
- **Verfügbarkeit**: Gewährleistung, dass Informationen und Systeme zuverlässig und termingerecht verfügbar sind, um die Geschäftskontinuität und Servicequalität zu sichern.

Diese Grundsätze stehen in direkter Verbindung mit unseren Unternehmenszielen. Die Wahrung der Vertraulichkeit schützt unsere Wettbewerbsvorteile und stärkt das Vertrauen von Kunden und Partnern. Die Integrität ermöglicht stabile, nachvollziehbare Prozesse und minimiert operative Risiken. Die Verfügbarkeit unterstützt eine unterbrechungsfreie Leistungserbringung sowie unsere Innovationskraft und Marktposition.

Unser Ziel ist es, Informationssicherheit nicht nur als technische Notwendigkeit, sondern als strategischen Erfolgsfaktor zu begreifen – und sie als solchen nachhaltig in allen Bereichen der Organisation zu verankern.

3.4 ISMS-Ziele

Ziele des Informationssicherheitsmanagementsystems sind insbesondere:

- Die Erfüllung aller Anforderungen der ISO/IEC 27001, insbesondere eine erfolgreiche (Re)-Zertifizierung,
- die Einführung und regelmäßige Durchführung von ISMS-Training und Sensibilisierungsmaßnahmen zur Steigerung der Informationssicherheitskompetenz aller Mitarbeitenden,
- das Gesamtrisiko der Organisation im Sinne der Informationssicherheit soll maximal "Mittel" sein.

Die Ziele des ISMS werden dokumentiert und deren Erfüllung gemäß Kapitel 3.7 überprüft.

3.5 Begründung für Aufbau und Betrieb eines ISMS

Der Aufbau eines ISMS basiert auf folgenden Motiven:

- Schutz sensibler Daten und Geschäftsprozesse: Unsere Informationen sind ein wertvolles Kapital. Ihr Schutz vor Verlust, Manipulation oder unberechtigtem Zugriff ist essenziell.
- Gesetzliche und regulatorische Anforderungen: Ein ISMS hilft uns, gesetzliche Vorgaben (z. B. DSGVO, BSI-Gesetz, ISO/IEC 27001) systematisch und nachweisbar zu erfüllen.
- Vertrauen von Kunden und Partnern: Informationssicherheit stärkt das Vertrauen in unser Unternehmen, insbesondere bei der Zusammenarbeit mit sicherheitsbewussten Partnern.
- Risiko- und Reputationsmanagement: Ein funktionierendes ISMS identifiziert Risiken frühzeitig und minimiert potenzielle Schäden durch Sicherheitsvorfälle.

3.6 Beitrag des ISMS zur Erreichung der Unternehmensziele

Ein ISMS trägt wesentlich zu unseren Unternehmenszielen bei, indem es:

- Geschäftskontinuität sicherstellt: Durch die frühzeitige Identifikation und Behandlung von Risiken wird der Geschäftsbetrieb stabil gehalten.
- Effizienz fördert: Klar definierte Prozesse und Zuständigkeiten reduzieren Reaktionszeiten im Ernstfall.
- Innovation absichert: Vertrauliche Projektdaten und geistiges Eigentum werden geschützt, was die Umsetzung neuer Ideen erleichtert.
- Wettbewerbsvorteile schafft: Eine nachweisbare Informationssicherheit nach internationalen Standards verbessert unsere Marktposition.

3.7 Planung und Überprüfung der Ziele der ISMS und ihrer Erfüllung

Bei der Planung, wie die Ziele des ISMS erreicht werden sollen, müssen die geplanten Maßnahmen, die Ressourcen, Verantwortlichkeiten, zeitlichen Ziele sowie die Bewertungsmethode für die Überprüfung festgelegt werden. Die Punkte sind zu dokumentieren. Die Ziele des ISMS und deren Erfüllung sind jährlich zu überprüfen. Verantwortlich für die Durchführung der Überprüfung, die Analyse der Ergebnisse der Überprüfung und die Erstellung eines Prüfberichts für das Management ist der Informationssicherheitsbeauftragte.

3.8 Informationssicherheitsmaßnahmen

Die Organisation verpflichtet sich, die geltenden Anforderungen an die Informationssicherheit zu erfüllen, wie sie in den themenspezifischen Informationssicherheitsrichtlinien des ISMS und ISO/IEC 27001 definiert sind. Geeignete Informationssicherheitsmaßnahmen (sogenannte Controls) werden innerhalb des Risikomanagementrahmens in der Methodik zur Risikobewertung und Risikobehandlung identifiziert, definiert und überprüft.

Die anwendbaren Informationssicherheitsmaßnahmen, ihr Umsetzungsstatus und etwaige Ausnahmen werden in der Erklärung zur Anwendbarkeit (sogenannte Statement of Applicability (SOA)) dokumentiert. Verantwortlich für die SOA ist der Informationssicherheitsbeauftragte. Die SOA ist gemäß dem Kapitel "Verwaltung von Aufzeichnungen zu diesem Dokument" abzulegen.

4. Verantwortlichkeiten

Im Rahmen des ISMS gibt es folgende Verantwortlichkeiten:

Stellenbezeichnung	**Verantwortlich für**
Vorstand	die korrekte Umsetzung und Instandhaltung des ISMS gemäß der Informationssicherheitsleitlinie sowie die Sicherstellung, dass ausreichend Ressourcen dafür verfügbar sind.
Informationssicherheits-beauftragter	die Koordination des Betriebs des ISMS und die Berichterstattung über dessen Leistungsfähigkeit.
Informationssicherheits-beauftragter	die Sicherstellung, dass jährliche Überprüfungen des ISMS bzw. bei entscheidenden Änderungen durchgeführt und protokolliert werden.
Informationssicherheits-beauftragter	das Informationssicherheitsbewusstsein aller Mitarbeiter sowie deren Ausbildung und Schulung zum Thema Informationssicherheit.
Asset-Owner	die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit der Assets bzw. Informationen, für die die Person zuständig ist.
Alle Mitarbeiter	die Meldung von Informationssicherheitsvorfällen oder Schwachstellen.
Informationssicherheits-beauftragter	die Behandlung von Informationssicherheitsvorfällen und Schwachstellen.
Vorstand	die Definition der Informationen, die im Rahmen der Informationssicherheit an interessierte Parteien kommuniziert werden.

Alle wesentlichen Verantwortlichkeiten und wiederkehrenden Aufgaben im ISMS werden über den Task Manager im Digital Compliance Office (DCO) gesteuert und dokumentiert.

5. Unternehmenspolitik

Die Informationssicherheit ist auf der obersten Führungsebene der Organisation verankert. Der Vorstand hat sich dem ISMS gemäß den Anforderungen von ISO/IEC 27001 und den Anforderungen des Risikomanagements verpflichtet, um das System an die sich ständig ändernden Geschäftsbedingungen anzupassen und sicherzustellen, dass die erforderlichen Ressourcen bereitgestellt werden. Dies soll alle relevanten Beteiligten des ISMS in die Lage versetzen, die Ziele der Informationssicherheit zu erreichen und das ISMS kontinuierlich zu verbessern. Der Vorstand ist auch für die Umsetzung der Unternehmenspolitik verantwortlich.

6. Verpflichtungen und Zuständigkeiten im Bereich der Informationssicherheit

Alle Mitarbeitende und relevante Dritte müssen mit der Informationssicherheitsleitlinie der Organisation und dem ISMS vertraut sein. Alle Mitarbeitende müssen in Übereinstimmung mit der Informationssicherheitsleitlinie, den themenspezifischen Informationssicherheitsrichtlinien und allen von dem Vorstand festgelegten Vorgaben handeln. Sofern gegen Unternehmensrichtlinien verstoßen wird, können disziplinarische Maßnahmen eingeleitet werden. Der Vorstand ist dafür verantwortlich, die Informationssicherheitsleitlinie zu kommunizieren und die Bedeutung des ISMS und der unternehmensweiten Verpflichtung zur Informationssicherheit zu verdeutlichen.

7. Referenzdokumente

Die folgenden Dokumente werden referenziert:

- Anwendungsbereich des ISMS
- Verfahren zur Identifikation von Erfordernissen
- Verfahren zu Informationssicherheitszielen & KPIs
- Verfahren zur Korrekturmaßnahmen

8. Verwaltung von Aufzeichnungen zu diesem Dokument

Folgende Aufzeichnungen werden zu diesem Dokument geführt:

- Übersicht der ISMS-Ziele & KPIs
- Bericht ISMS & KPI Zielerreichung
- Managementbewertung
- Berufung ISB
- Ressourcenplanung
- Übersicht rechtlicher, amtlicher, vertraglicher und anderer Erfordernisse
- Statement of Applicability (SOA) / VDA ISA catalogue

Die Aufzeichnungen sind gemäß dem Verfahren zur Lenkung von Dokumenten und Aufzeichnungen aufzubewahren.

9. Gültigkeit und Dokumentenhandhabung

Dieses Dokument ist gültig ab 01.11.2025.

Der Eigentümer dieses Dokuments ist der Informationssicherheitsbeauftragte, der das Dokument mindestens einmal jährlich prüfen und gegebenenfalls aktualisieren muss.

Für die Auswertung des Dokuments auf Wirksamkeit und Angemessenheit sowie möglichen Anpassungsbedarf müssen mindestens folgende Kriterien berücksichtigt werden:

- Ergebnisse von internen und externen Audits
- Ergebnisse der KPI-Auswertung
- Ergebnisse der Managementbewertung
- Anpassungen, die sich aus dem Risiko-Management oder Korrekturmaßnahmen ergeben