ÜBERGEORDNETE LEITLINIE NACH ISO 27001 UND DSGVO

Version: 2.4

Erstelldatum: 17.08.2017
Ersteller: Oliver Thehos

DOKUMENTENLENKUNG

Klassifizierung 1-10 (wichtig)	10
Klassifizierung 1-10 (vertraulich)	1
Titel	Übergeordnete Leitlinie ISMS und Datenschutz
Definitiver Speicherort	[Speicherort, z.B. URL der Datei auf einem Dateiserver oder in einem Dokumentenmanagementsystem]
Verantwortlicher	Oliver Thehos - Vithos Consulting
Version	2.4
Datum der letzten Änderung	15.02.2018
Nächstes Review bis	01.08.2018
Versions- und Änderungshistorie	Siehe Change Management

CHANGE MANAGEMENT

Version	Datum	Kommentar
1.0	17.08.2017	Version zur Diskussion
2.0	28.10.2017	Version inkl. DSGVO Leitlinie
2.1	26.01.2018	Version zur Prüfung durch die Geschäftsführung
2.2	01.02.2018	Version zur Überprüfung durch die Geschäftsführung
2.3	07.02.2018	Version inkl. Unterschriftsfeld
2.4	15.02.2018	Anpassung - einführender Satz zur Dokumentenlenkung

INHALTSVERZEICHNIS

1 EINFÜHRUNG, ZIELE & ZIELGRUPPEN

1.1 Einführung

Dieses Dokument beschreibt die Richtlinie für die Informationssicherheit des Informationssicherheitsmanagementsystems (ISMS) im geltenden Anwendungsbereich und damit die Informationssicherheits- und Datenschutzziele der Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG.

Die Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG (nachstehend HiSV genannt) ist ein führendes Beratungsunternehmen für Sportversicherungen in Deutschland und Kontinentaleuropa.

HiSV wurde in den 50er Jahren von Erwin Himmelseher als Familienunternehmen gegründet. Die Kunden schätzen insbesondere die Qualität der Arbeit, den persönlich, vertrauensvollen Kontakten zu ihren Ansprechpartnern und die stringenten Entscheidungsprozesse.

Das Vertrauen der Kunden in die außergewöhnliche Dienstleistung ist das Kapital von HiSV und alle aufgeführten Absichten, Maßnahmen und Selbstverpflichtungen in dieser Leitlinie dienen dem Ziel, die Werte von HiSV und die ihnen anvertrauten personenbezogenen Daten ihrer Kunden und Partner zu schützen.

1.2 Ziele

Die Firmenphilosophie hinsichtlich des nachhaltigen Schutzes von Informationen sowie des sensiblen und rechtskonformen Umgangs bei der Verarbeitung von personenbezogenen Daten nimmt in dieser Leitlinie bei der Ausrichtung des ISMS und bei Priorisierung von Maßnahmen und Geschäftsprozessen seitens aller Mitarbeiter und Partner von HiSV eine übergeordnete und richtungsweisende Rolle ein.

Das Ziel ist ein angemessener und wirksamer Schutz der potenziell kritischen Infrastrukturen, Systeme, Anwendungen und Informationen mit Hilfe eines ISO 27001 zertifizierten ISMS, um die Anforderungen unserer Kunden, Partner und gesetzlichen Vorgaben, speziell des BDSV (Bundesdatenschutzverordnung), zu erfüllen.

Die Geschäftsführung von HiSV gibt durch die Einführung eines ISMS nach ISO 27001 zur Steuerung und kontinuierlichen Verbesserung der Informationssicherheit und des Datenschutzes eine klare Richtung zur normierten Einhaltung dieser Grundsätze in Einklang mit den Geschäftszielen und der Unternehmensphilosophie vor.

2 GELTUNGSBEREICH & GRENZEN

Die Leitlinie zur Informationssicherheit und Datenschutz und die damit verbundenen Dokumente gelten für alle Mitarbeiter von HiSV.

Unsere Dienstleister werden zur Einhaltung der nachfolgenden Anforderungen verpflichtet. Vertragspartner werden auch aufgrund der Umsetzung der Datenschutzvorgaben und der transparenten Informationssicherheitsmechanismen ausgewählt.

3 GESETZE, NORMEN, STANDARDS UND VORGABEN

Die Einhaltung der relevanten Gesetze, Normen, Vorschriften und Anforderungen aus Verträgen werden eingehalten und erfahren durch unsere internen und externen Audits einen regelmäßigen Review.

Die Änderungen werden regelmäßig bewertet und im Zuge der kontinuierlichen Verbesserung eingearbeitet.

Folgende Vorgaben sind zu berücksichtigen:

- Bundesdatenschutzgesetz, EU- Datenschutzgesetz
- Bereitstellung eines Sicherheitskonzepts nach §9 – techn. und organisatorische Maßnahmen; Sorgfalt hinsichtlich Persönlichkeitsrechten Betroffener, Datensparsamkeit, Vertraulichkeit
- ISO/IEC 27001
- Bereitstellung eines Informationssicherheitsmanagementsystems zur Steuerung von Datenschutz und Informationssicherheitsvorgaben
- Verträge mit Kunden und Partnern
- GDPdU, GOBS
- Sorgfaltspflichten bei der Verarbeitung, Vorhaltung und Bereitstellung von Informationen, insbesondere zu rechnungsrelevanten Daten zur Buchführung und Steuerprüfung; Forderung zur Einrichtung eines internen Kontrollsystems
- Vertraulichkeitserklärungen mit Geschäftspartnern (Kunden, Dienstleistern und Partnern)

4 INFORMATIONSSICHERHEIT – ALLGEMEIN

Unsere maßgeblichen Sicherheitskriterien sind Verfügbarkeit, Vertraulichkeit und Integrität.

Vertraulichkeit: Informationen werden gegenüber unberechtigten Personen oder Entitäten nicht offengelegt.

Integrität: Die Vollständigkeit und Korrektheit/Unverfälschtheit von Informationswerten wird geschützt.

Zugreifbarkeit/Verfügbarkeit: Berechtigte Personen oder Entitäten können auf Informationen zugreifen und diese nutzen, wann immer dies erforderlich ist.

Die Maßnahmen zur Umsetzung der Sicherheitskriterien und das Erreichen der Sicherheitsziele sind in erster Linie nicht technischer, sondern organisatorischer Natur. Hierzu haben wir ein Informationssicherheitsmanagementsystem (ISMS) nach der Norm ISO/IEC 27001 eingeführt.

Das ISMS unterstützt HiSV, die Informationssicherheit und die Datenschutzvorgaben strukturiert zu managen. Es umfasst die Einrichtung, Implementierung, Betrieb, Überwachung, Review, Wartung und Verbesserung der Informationssicherheit und stützt sich auf das nachhaltige Management von Geschäftsrisiken.

Da Informationssicherheit und Datenschutz kein starres Ziel ist, sondern aufgrund verschiedenster Umstände (Kundenanforderungen, Gesetzesänderungen etc.) ein dynamischer, fortwährender Prozess, gilt für uns der Grundsatz der ständigen Verbesserung mithilfe des PDCA-Zyklus:

5 BEDEUTUNG DER INFORMATIONSSICHERHEIT

Alle Mitarbeiter von HiSV, Partner und Dienstleister müssen sich zur Einhaltung des Datenschutzes und der Informationssicherheit unter Berücksichtigung dieser Leitlinie bekennen, da unseren Kunden den Schutz der Vertraulichkeit, der Integrität und Verfügbarkeit erwarten und Verstöße unseren Kunden und uns signifikanten Schaden zufügen können.

Daher liegt es in der Verantwortung aller Mitarbeiter, Partner und Dienstleister Verstöße gegen die genannten Normen zu vermeiden und ggf. Verbesserungsvorschläge zur Verhinderung von Datenschutz- und Informationssicherheitsvorfällen dem ISMS- oder Datenschutzbeauftragten aufzuzeigen.

6 KONTROLLEN & SANKTIONEN

Die Einhaltung der Vorgaben aus dem Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001 werden regelmäßig oder anlassbezogen mit Hilfe eines Auditprogramms überprüft.

Verstöße gegen die Vorgaben werden verfolgt und entsprechend geahndet.

7 BEKENNTNIS DER GESCHÄFTSFÜHRUNG

Diese Leitlinie zum Datenschutz und zur Informationssicherheit wird von der Geschäftsführung freigegeben.

Die Geschäftsführung bekennt sich zu dieser Richtlinie, zur Einhaltung der Datenschutzvorgaben und zum Informationssicherheitsmanagement insgesamt und stellt die entsprechenden personellen, organisatorischen und finanziellen Mittel bereit, um das ISMS im Unternehmen wirkungsvoll und angemessen zu betreiben und zu verbessern.

In regelmäßigen Management Reviews wird das ISMS auf seine Wirksamkeit und Angemessenheit geprüft und verbessert.

Die Geschäftsführung unterstützt und engagiert sich für Informationssicherheit durch die organisationsweite Veröffentlichung, Durchsetzung und Aufrechterhaltung dieser und weiterer ISMS-Richtlinien als auch bei der Kontrolle und Weiterentwicklung des ISMS unter Aufbietung aller geforderten Ressourcen zur Erreichung der organisatorischen und technischen Maßnahmen und Ziele.

8 WICHTIGE ROLLEN UND VERANTWORTLICHKEITEN

8.1 Eigenverantwortung

Jeder Mitarbeiter ist verpflichtet, die Prozesse von HiSV zur Aufrechterhaltung der Informationssicherheit zu befolgen. Des Weiteren ist er für die ihm im Rahmen seiner Aufgaben und Projekte, etc. anvertrauten Informationen verantwortlich. Ein Mitarbeiter kann hier mehrere Rollen einnehmen, Rollen können auch an externe Fachkräfte ausgelagert werden.

8.2 Chief Information Security Officer (Informationssicherheitsbeauftragter)

Der Information Security Officer wurde von der Geschäftsführung benannt. Diese Rolle stellt sicher, dass das Informationssicherheitssystem (ISMS) im Unternehmen entsprechend der Vorgaben der Geschäftsführung etabliert, betrieben und verbessert wird.

8.3 Datenschutzbeauftragter

Der Datenschutzbeauftragte wurde von der Geschäftsführung benannt. Er unterstützt den Information Security Officer bei der Erfüllung seiner Aufgaben und ist Anlaufstelle für datenschutzbezogene Fragen und Anliegen.

8.4 Risikomanager (Risk Manager)

Der Risikomanager ist für die Planung, Umsetzung, Überwachung und Verbesserung des Risikomanagements in der IT Service Management Organisation verantwortlich. Er etabliert dazu einen entsprechenden Risikomanagementprozess, mit dem die Risiken einer Organisation identifiziert, analysiert und bewertet werden. Festlegung der mit dem Management abgestimmten Risikoakzeptanzkriterien.

8.5 Risikoeigentümer (Risk Owner)

Die eingesetzten Risikoeigentümer sind für alle Auswirkungen und damit auch für die Behandlung, Akzeptanz und Überwachung eines oder mehrerer IT-Risiken verantwortlich. Sie überprüfen regelmäßig die Wirksamkeit der Behandlungsmaßnahmen.

8.6 Asset Owner

Für jeden unterstützten informationsverarbeiteten Geschäftsprozess werden unterschiedliche Assets (Werte) zur Unterstützung benötigt. Folgende Asset-Gruppen sind zum Beispiel vorgesehen:

- Informationen (alle)
- Business und unterstützende (IT) Services
- Hardware/Software
- Vermögenswerte
- Reputation und Ansehen

8.7 Prozessverantwortlicher (Process Owner)

Der Prozessverantwortliche ist für die Definition der Prozessziele, Kennzahlen und Richtlinien, für die Bereitstellung der entsprechenden Ressourcen sowie für die Kontrolle der Zielerreichung verantwortlich.

8.8 Prozessmanager

Der Prozessmanager ist für die Effektivität und Effizienz des Gesamtprozesses verantwortlich und berichtet an den Prozessverantwortlichen

9 RISIKOMANAGEMENT

Das Risikomanagement wird für die nachhaltige Risikovermeidung und proaktiven Risikosteuerung etabliert, um die negativen Auswirkungen auf die Geschäftsprozesse im richtigen Kontext beurteilen zu können und den richtigen Umgang mit IT-Risiken, Informationssicherheit und datenschutzrelevanten Themen sicherzustellen.

9.1 Informationsklassifizierung

Die Informationsklassifizierung erfolgt nach den Empfehlungen der ISO/IEC 27007 8.2.1 durch den Risk Owner:

Informationen sollten nach Ihrem Wert, gesetzlichen Vorschriften, Betriebswichtigkeit uns Sensibilität im Hinblick auf unbefugte Offenlegung oder Veränderung klassifiziert werden

- Grundsätzlich ist jede festgestellte (signifikante) Information ein schützenswertes Gut. Wir haben uns für die analytische Vorgehensweise mit folgenden Charakteristiken entschieden:
- Inventarisierung der Informationen zum Anwendungsbereich (einschließlich tangierender Bereiche)
- Klare Zuordnung von Verantwortlichen zur Information
- Risikobetrachtung und Schutzmaßnahmen werden möglichst nahe zur Information entwickelt und in Einklang mit den Vorgaben dieser Policy gebracht
- Kann dem Schutzbedürfnis einer Information durch Maßnahmen auf einer höheren Modellierungsebene wirkungsvoll Genüge getan werden, so haben diese Vorrang
- Aus diesem Grunde ist die Inventarisierung so zu modellieren, dass der Betrieb des ISMS mit Sicherheitsmaßnahmen angemessen erfolgen kann

9.2 Risikoakzeptanzkriterien

Das ISMS soll zu größerer Handlungssicherheit verhelfen und auch den Prozess der Beschäftigung mit Risiken effizienter gestalten (Recherchen vertiefen oder Risiko akzeptieren).

Das Verhältnis von Aufwand und Risikoreduktion soll für den entsprechenden Schutzbedarf des Anwendungsbereichs angemessen sein; entsprechend ist ein strategisches Risikomanagement installiert, das Maßnahmen an den Leitlinien ausrichtet und konform hält.

Als Bewertungsgrundlage richten wir uns nach der ISO 27005 und definieren hier drei Risikobereiche:

- 0-2 als „low risk“
- 3-5 als „medium risk“
- 6-8 als „high risk“

Laut Definition werden Risiken mit „low risk“ nicht spezifisch behandelt, sondern nur dessen Ausschluss begründet.

Alle anderen Risiken werden nach der Norm ISO 27001 und Anhang und ggf. nach Maßnahmen der ISO 27002 behandelt und dokumentiert.

Das Risiko kann und wird ausschließlich durch den Risk Owner und/oder das Top-Management akzeptiert.

10 INFORMATIONSSICHERHEITSEREIGNISSE UND -VORFÄLLE

Ein Informationssicherheitsereignis ist jedes Ereignis, das sicherheitsrelevant sein könnte. Jedes (potenzielle) Informationssicherheitsereignis muss gemeldet werden. Der Meldeweg sollte der Kritikalität des Ereignisses sowie der zeitlichen Dringlichkeit einer Reaktion entsprechend angemessen gewählt werden. Bei weniger kritischen Ereignissen soll eine E-Mail an security@himmelseher.com gesendet werden. In anderen Fällen soll der Service Desk telefonisch alarmiert werden.

Die externe Kommunikation von Sicherheitsvorfällen und damit verbundenen Ereignissen, Situationen oder Aktivitäten muss sowohl durch den ISMS-Beauftragten und den Datenschutzbeauftragten als auch der Geschäftsführung koordiniert werden. Mitarbeiter sind nicht befugt, Informationen im Zusammenhang mit Informationssicherheitsvorfällen herauszugeben.

11 INFORMATIONSSICHERHEITSBEWUSSTSEIN UND -SCHULUNGEN

Alle Mitarbeiter müssen an einer Grundlagen-Schulung zum Thema Sicherheitsbewusstsein teilnehmen und ein Online-Training zum Thema Datenschutz und Informationssicherheit absolvieren. Im Weiteren finden regelmäßig themenspezifische Awareness-Trainings statt.

12 SPEZIFISCHE SICHERHEITSRICHTLINIEN

Diese generelle Informationssicherheits-Richtlinie wird durch diverse themenspezifische Sicherheitsrichtlinien ergänzt und unterstützt. Jeder Mitarbeiter sollte diese Richtlinien anwenden und einhalten, insofern sie für seine Rolle und Position im Unternehmen relevant sind.

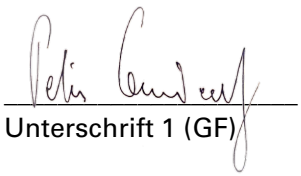
13 DOKUMENTENLENKUNG

Eine allgemeingültige Dokumentenlenkung wurde bereits entwickelt. Bis auf Widerruf werden alle ISO 27001 und datenschutzrelevanten Dokumente wie unten gekennzeichnet.

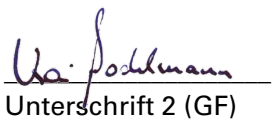
Klassifizierung 1-10 (wichtig)	10
Klassifizierung 1-10 (vertraulich)	1
Titel	Übergeordnete Leitlinie ISMS und Datenschutz
Definitiver Speicherort	[Speicherort, z.B. URL der Datei auf einem Dateiserver oder in einem Dokumentenmanagementsystem]
Verantwortlicher	Oliver Thehos- Vithos Consulting
Version	1.0
Datum der letzten Änderung	01.02.2018
Nächstes Review bis	01.03.2018
Versions- und Änderungshistorie	Version zur Vorlage bei der Geschäftsführung

Die Leitlinie zum Datenschutz und zur Datensicherheit tritt mit sofortiger Wirkung in Kraft.

Köln, den 15.02.2018



Unterschrift 1 (GF)



Unterschrift 2 (GF)