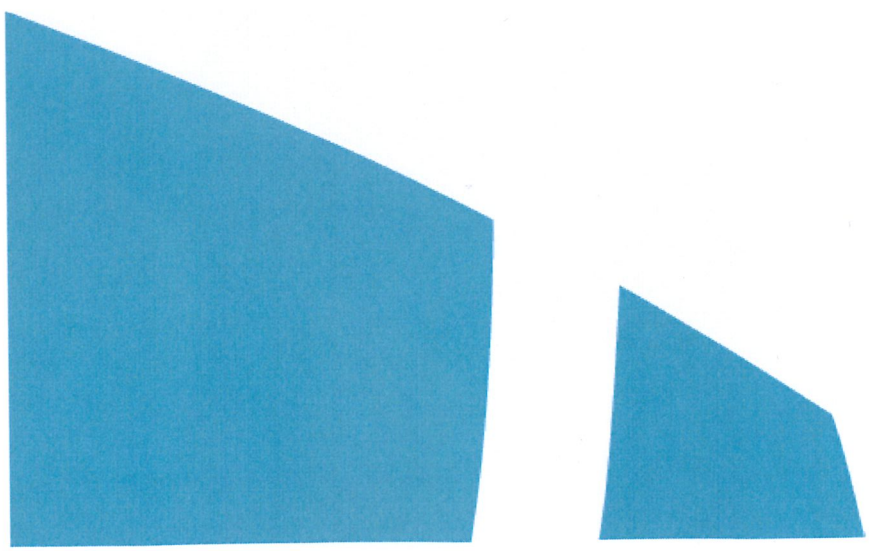
HiSV HIMMELSEHER Sportversicherung

GENERAL GUIDELINE ACCORDING TO ISO 27001 AND GDPR

Version: 2.4

Date created: 17.08.2017

Author: Oliver Thehos



HiSV HIMMELSEHER Sportversicherung

TABLE OF CONTENTS

1 INTRODUCTION, AIMS & TARGET GROUPS 3
1.1 Introduction 3
1.2 Aims 4
2 SCOPE & LIMITS 5
3 ACTS, NORMS, STANDARDS AND REQUIREMENTS 6
4 Information SECURITY – GENERAL 7
5 SIGNIFICANCE OF INFORMATION SECURITY 8
6 CONTROLS & SanCtionS 8
7 COMMITMENT OF MANAGEMENT 9
8 IMPORTANT ROLES AND RESPONSIBILITIES 10
8.1 Personal responsibility 10
8.2 Chief information security officer 10
8.3 Data protection officer 10
8.4 Risk manager 10
8.5 Risk owner 10
8.6 Asset owner 10
8.7 Process owner 10
8.8 Process manager 11
9 Risk management 12
9.1 Information classification 12
9.2 Risk acceptance criteria 13
10 Information SECURITY EVENTS AND INCIDENTS 14
11 Information SECURITY AWAREHNESS AND TRAINING 14
12 SpeCIFIC SECURITY GUIDELINES 14
13 Document control 15

1 INTRODUCTION, AIMS & TARGET GROUPS

1.1 Introduction

This document describes the Guideline for the Information Security Management System (ISMS) in the applicable area of application and therefore the information security and data protection aims of Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG.

Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG (referred to in the following as HiSV) is a leading consultancy for sports insurance in Germany and continental Europe.

HiSV was founded in the fifties by Erwin Himmelseher as a family company. The clients appreciate in particular the quality of work, the personal and trustful contacts and the stringent decision-making processes.

The trust of clients in the extraordinary service is HiSV's capital and all intentions, measures and self-commitments in this Guideline serve the objective of protecting HiSV's assets and the personal data with which it has been entrusted by its clients and partners.

1.2 Aims

The corporate philosophy regarding the sustainable protection of information and the sensitive and legally compliant approach to processing personal data assumes an overriding and indicative role in this Guideline in the orientation of the ISMS and the prioritisation of measures and business processes on the part of all employees and partners of HiSV.

The aim is to achieve a suitable and effective protection of the potentially critical infrastructures, systems, applications and information with the assistance of an ISO 27001-certified ISMS in order to meet the requirements of our clients, partners and the law, in particular the Federal Data Protection Ordinance (BDSV - *Bundesdatenschutzverordnung*).

Through the introduction of an ISMS in accordance with ISO 27001 to control and continuously improve information security and data protection, the management of HiSV gives a clear direction for the standardised compliance with these principles in line with business objectives and the corporate philosophy.

2 SCOPE & LIMITS

The Guideline on Information Security and Data Protection and the associated documents apply to all HiSV employees.

Our service providers are obligated to observe the following requirements. Contracting partners are also selected on the basis of the implementation of data protection requirements and transparent information security mechanisms.

3 ACTS, NORMS, STANDARDS AND REQUIREMENTS

The relevant acts, norms, standards, provisions and contractual requirements are observed and are regularly reviewed in internal and external audits.

Changes are regularly assessed and incorporated as part of the continuous improvement process.

The following requirements are to be considered:

- Federal Data Protection Act, EU Data Protection Act
- Provision of a security concept in accordance with Section 9 – technical and organisational measures; care with respect to the personal rights of data subjects, data economy, confidentiality
- ISO/IEC27001
- Provision of an Information Security Management System to control data protection and information security requirements
- Agreements with customers and partners
- GDPdU (principles of data access and the auditability of digital documents), GOBS (principles of correct IT-supported bookkeeping systems)
- Duties to take care in the processing and provision of information, in particular invoice-relevant data for bookkeeping and tax audits; demand for the establishment of an internal control system
- Declarations of confidentiality with business partners (clients, service providers and partners)

4 INFORMATION SECURITY – GENERAL

Our guiding security criteria are availability, confidentiality and integrity.

Confidentiality: information is not disclosed to unauthorised individuals or entities.

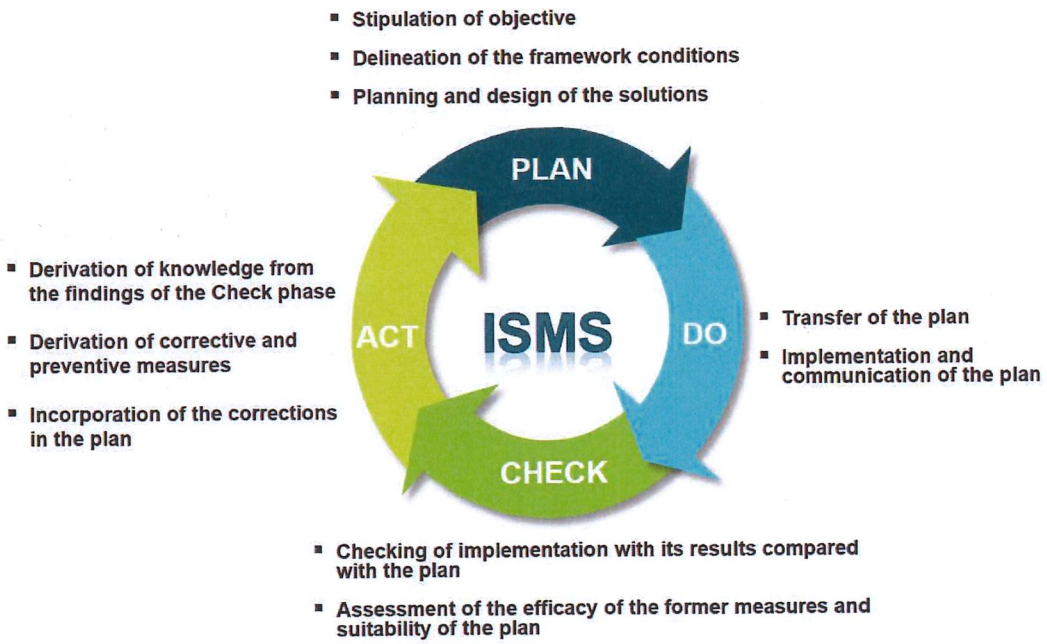
Integrity: the completeness and correctness/authenticity of information assets are protected.

Accessibility/availability: authorised individuals or entities can have access to and use information whenever this is necessary.

The measures to implement security criteria and to achieve security goals are not primarily technical but rather organisational. For this purpose, we have introduced an Information Security Management System (ISMS) in accordance with ISO/IEC 27001.

The ISMS supports HiSV in managing information security and data protection requirements in a structured manner. It comprises the establishment, implementation, operation, monitoring, review, service and improvement of information security and is based on the sustainable management of business risks.

Since information security and data protection are not rigid objectives but are a dynamic and ongoing process due to a broad variety of circumstances (customer requirements, changes in the law etc.), we apply the principle of constant improvement using the PDCA cycle:



5 SIGNIFICANCE OF INFORMATION SECURITY

All employees of HiSV, partners and service providers must commit to observing data protection and information security under consideration of this Guideline because our clients expect protection of confidentiality, integrity and availability and any breaches could significantly damage our clients and us.

It is therefore the responsibility of all employees, partners and service providers to avoid breaches of the specified norms and to indicate any suggested improvements to prevent data protection and information security incidents to the ISMS or data protection officer.

6 CONTROLS & SANCTIONS

Compliance with the requirements of the Information Security Management System (ISMS) under ISO/IEC 27001 is checked on a regular or ad hoc basis with the assistance of an audit programme.

Infringements of the requirements are pursued and punished accordingly.

7 COMMITMENT OF MANAGEMENT

This Guideline on Data Protection and Information Security is approved by management.

Management is committed to this Guideline, to complying with the data protection requirements and information security management in its entirety and provides the corresponding staffing, organisational and financial means to effectively and suitably operate and improve the ISMS in the company.

The ISMS is checked for efficacy and appropriateness and improved in regular management reviews.

Management supports and engages with information security through company-wide publication, assertion and maintenance or this and further ISMS Guidelines and in the control and further development of the ISMS, mobilising all requisite resources to achieve the organisational and technical measures and aims.

8 IMPORTANT ROLES AND RESPONSIBILITIES

8.1 Personal responsibility

Every employee is obliged to observe the processes of HiSV to uphold information security. Furthermore, every employee is responsible for the information provided to them for their tasks and projects. An employee can assume several roles here. Roles can also be outsourced to external qualified persons.

8.2 Chief information security officer

The information security officer has been appointed by management. This role ensures that the information security system (ISMS) is established, operated and improved in the company in accordance with management requirements.

8.3 Data protection officer

The data protection officer has been appointed by management. He supports the information security officer in the satisfaction of his tasks and the point of contact for questions and matters related to data protection.

8.4 Risk manager

The risk manager is responsible for the planning, implementation, monitoring and improvement of risks management in the IT service management organisation. For this purpose, he establishes a suitable risk management process with which the risks of an organisation are identified, analysed and assessed. Stipulation of the risk acceptance criteria agreed with management.

8.5 Risk owner

The risk owners are responsible for all effects and therefore also for the treatment, acceptance and monitoring or one or several IT risks. They regularly check the efficacy of the treatment methods.

8.6 Asset owner

Different assets are required to support every supported information-processing business process. The following asset groups are envisaged, for example:

- Information (all)
- Business and supporting (IT) services
- Hardware/software
- Financial assets
- Reputation and image

8.7 Process owner

The Process owner is responsible for defining process objectives, ratios and guidelines, for the provision of corresponding resources and for checking the achievement of objectives.

8.8 Process manager

The process manager is responsible for the effectiveness and efficiency of the entire process and reports to the process owner.

9 RISK MANAGEMENT

Risk management is established for sustainable risk avoidance and proactive risk control in order to assess the negative effects on the business processes in the right context and to ensure the correct handling of IT risks, information security and subjects of relevance to data protection.

9.1 Information classification

Information is classified by the risk owner in accordance with the recommendations in ISO/IEC 27007 8.2.1:

Information should be classified in accordance with its value, statutory provisions, importance to operations and sensitivity with respect to unauthorised disclosure or change

- In principle, every (significant) piece of information determined is a good which is worthy of protection. We have decided in favour of the analytical approach with the following characteristics:
- Inventory of information on the scope (including affected areas)
- Clear assignment of owners to information
- Risk assessment and protective measures are developed as near to the information as possible and aligned with the requirements of this policy
- If the protection requirement of a piece of information can be effectively satisfied by measures at a higher modelling level, they take priority
- For this reason, the inventory is to be modelled such that the ISMS can be suitably implemented with security measures

9.2 Risk acceptance criteria

The ISMS is intended to contribute to greater security of action and to efficiently shaping the process of dealing with risks (deepen research or accept risk).

The relationship between expense and risk reduction should be appropriate to the corresponding need to protect the area of application; accordingly, strategic risk management is installed which aligns measures to the guidelines and keeps them compliant.

We are guided by ISO 27005 as assessment foundation and define three risk areas here:

- 0-2 as "low risk"
- 3-5 as "medium risk"
- 6-8 as "high risk"

According to the definition, low risks are not dealt with specifically but only their exclusion justified.

All other risks are treated and documented in accordance with ISO 27001 and Annex and any measures in accordance with ISO 27002.

The risk can and is accepted exclusively by the risk owner and/or top management.

10 INFORMATION SECURITY EVENTS AND INCIDENTS

An information security event is any event which could be of relevance to security. Every (potential) information security event must be reported. The reporting path should be suitably selected in accordance with the criticality of the event as well as the temporal urgency of a reaction. With less critical events an email should be sent to security@himmelseher.com. In other cases, the Service Desk should be alerted by telephone.

The external communication of security incidents and the associated events, situations or activities must be coordinated both by the ISMS officer and the data protection officer as well as management. Employees are not authorised to issue information in connection with information security incidents.

11 INFORMATION SECURITY AWAREHNESS AND TRAINING

All employees must participate in basic training on the subject of security awareness and must pass online training on the subject of data protection and information security. Subject-specific awareness training also takes place at regular intervals.

12 SPECIFIC SECURITY GUIDELINES

This general Information Security Guideline is supplemented and supported by subject-specific guidelines. Every employee should use and comply with these guidelines where they are of relevance to their role and position in the company.

13 DOCUMENT CONTROL

Generally valid document control has already been developed. Until further notice, all ISO 27001 documents and those of relevance to data protection will be marked as shown below as an example.

Classification 1-10 (important)	10
Classification 1-10 (confidential)	1
Title	General Guideline ISMS and Data Protection
Definitive storage site	[Storage site, e.g.URL of the file on a file server or in a document management system]
Controller	Oliver Thehos- Vithos Consulting
Version	1.0
Date of last change	01.02.2018
Next review by	01.03.2018
Version and change history	Version for submission to management

The Guideline on Data Protection and Data Security enters into force with immediate effect.

Cologne, 19.07.2021

Signature 1 (Managing Director)

Signature 2 (Managing Director)