Leitlinie Informationssicherheit

Inhaltsverzeichnis

1 Referenzen zu Standards

Die folgende Tabelle zeigt die Referenzen zum Standard ISO/IEC 27001:2013.

Thema	**ISO 27001:2013**
Leitlinie	#5.2
Informationssicherheitsrichtlinien	A.5.1.1
Überprüfung der Informationssicherheitsrichtlinien	A5.1.2

2 Präambel

Die übergeordnete Leitlinie des Informationssicherheitsmanagementsystems (ISMS) beschreibt die Rahmenbedingungen im geltenden Anwendungsbereich und damit die Informationssicherheitsschutzziele der HEGENSCHEIDT-MFD.

3 Bekenntnis der Geschäftsführung

Als Hersteller hochwertiger Werkzeugmaschinen und Anlagen ist es für die HEGENSCHEIDT-MFD GmbH eine selbstverständliche Pflicht hinsichtlich Qualität, Umwelt, Informationssicherheit, Datenschutz, Arbeitssicherheit und Gesundheit für alle, die von diesem Prozess betroffen sind, mit besonderer Sorgfalt bei der Entwicklung neuer, marktgerechter Produkte, deren Konstruktion, Vertrieb, Produktion, Dienstleistung und Kundendienst vorzugehen.

Um diese Aufgabe und die damit verbundenen Zielsetzungen zu erfüllen, haben sich Geschäftsführung sowie alle Führungskräfte und Mitarbeiter des Unternehmens verpflichtet, nach dem Managementsystem gemäß ISO 9001, VDA 6.4, und ISO 14001 und ISO 27001 sowie allen rechtlichen Vorschriften für Umwelt, Arbeitssicherheit und Gesundheit sowie Datenschutz und Informationssicherheit zu arbeiten.

Die durch diese Normen vorgegebenen Managementsysteme haben wir in einem integrierten Management Handbuch dokumentiert und dieses zu einer verbindlichen Arbeitsgrundlage für alle strategischen und operativen Geschäftsprozesse erklärt. Alle Mitarbeiter des Unternehmens sind verpflichtet, nach diesen Grundsätzen zu handeln.

Indem finanzielle Verluste durch Sicherheitsvorfälle auf ein Minimum verringert werden, trägt das Informationssicherheitsmanagement positiv zum Geschäftsergebnis bei. Dadurch wird unser Ansehen als das eines vertrauenswürdig, offen, ehrlich und ethisch handelnden Unternehmens gefestigt.

Eine zuverlässige sichere Datenverarbeitung ist für den reibungslosen Ablauf eines Betriebes absolute Notwendigkeit. Unzureichender Schutz von Daten und Informationen, ob geschrieben, gesprochen oder digital, sind ein unterschätzter Risikofaktor, der unzureichend geschützt und nicht abgesichert, existenzbedrohende Ausmaße annehmen kann.

Die Geschäftsführung bekennt sich zu dieser Leitlinie, zur Einhaltung der Schutzziele 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.

4 Bedeutung der Informationssicherheit und des Datenschutzes

Alle HEGENSCHEIDT-MFD Mitarbeiter müssen sich zur Einhaltung des Datenschutzes und der Informationssicherheit unter Berücksichtigung dieser Leitlinie bekennen, da unsere 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, Verstöße gegen die genannten normativen und gesetzlichen Anforderungen zu vermeiden und bei Gefährdung oder Verletzung unverzüglich zu melden. Hierzu sind entsprechende Melde- und Eskalationswege definiert.
Verstöße gegen die Vorgaben werden verfolgt und entsprechend geahndet.

5 Geltungsbereich

Die Leitlinie zur Informationssicherheit und die damit verbundenen Dokumente gelten für alle Mitarbeiter von HEGENSCHEIDT-MFD. Unsere Lieferanten, Partner und Dienstleister werden zur Einhaltung der nachfolgenden Anforderungen verpflichtet. Der HEGENSCHEIDT-MFD Geltungsbereich wird im Dokument Kontext der Organisation ausführlich beschrieben.
Die Anwendbarkeit der normativen Anforderungen werden über die SOA (Statement of applicability) bestimmt.

6 Zuständigkeit (Verantwortlicher)

Umsetzungsverantwortlich ist der Informationssicherheitsbeauftragte.
Er steht auch für jegliche Rückfragen oder Anpassungsbedarf der Richtlinie zur Verfügung.

7 Leitlinie

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

Die Geschäftsführung von HEGENSCHEIDT-MFD 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.

Die Rahmenbedingungen des ISMS werden durch relevante Gesetze, Normen, Vorschriften und Anforderungen aus Verträgen gesetzt. Deren Einhaltung überprüft HEGENSCHEIDT-MFD in regelmäßigen Reviews sowie durch interne und externe Audits.

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

Die Geschäftsführung bildet das oberste Organ des Managementsystems innerhalb der HEGENSCHEIDT-MFD.

7.1 Zielsetzung

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

7.2 Schutzziele des ISMS

Die Maßnahmen der Informationssicherheit sind so gewählt, dass sie die Risiken im Umgang mit dem Geschäftswert Information handhabbar machen. Geschützt werden:

Vertraulichkeit
Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden, dies gilt sowohl beim Zugriff auf gespeicherte Daten wie auch während der Datenübertragung.

Integrität
Daten dürfen nicht unbemerkt verändert werden, respektive alle Änderungen müssen nachvollziehbar sein.

Verfügbarkeit
Verhinderung von Systemausfällen. Der Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet werden.

7.3 Selbstverständnis des ISMS

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

Das ISMS unterstützt die HEGENSCHEIDT-MFD, die Informationssicherheit 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 kein starres Ziel ist, sondern aufgrund verschiedenster Umstände ein dynamischer, fortwährender Prozess, gilt für uns der Grundsatz der ständigen Verbesserung mithilfe des PDCA-Zyklus.

7.4 Datenschutz allgemein

Ziel dieser Leitlinie ist es, Datenschutz im Unternehmen zu gewährleisten. Für diesen Zweck wird das Unternehmen bei der Planung, Einführung und während des Ablaufs von Prozessen nachfolgende Vorgaben bei der Verarbeitung von personenbezogenen Daten einhalten:

- Rechtmäßigkeit
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Verfügbarkeit und Belastbarkeit
- Verarbeitung nach Treu und Glauben („Fairness“)

Der Grundsatz der Rechenschaftspflicht verlangt den Nachweis der Einhaltung der o. g. Datenschutzgrundsätze, deren detaillierte Erklärung ein Teil der Richtlinie zum Datenschutz ist. Zur Erfüllung dieser Rechenschaftspflicht ist ein in sich stimmiges, systematisches und nachvollziehbares Datenschutzmanagement eingerichtet. Auf der Grundlage der diesbezüglich geführten Datenschutzdokumentation ist eine Überprüfung der Einhaltung dieser Grundsätze durch Datenschutzprüfungen und Audits möglich. Die in der Richtlinie zum Datenschutz zu diesem Zweck festgelegten Dokumentationen und Nachweise sind vollständig zu führen und aktuell zu halten.

7.5 Bewusstsein

7.5.1 Schulungen

Alle HEGENSCHEIDT-MFD Mitarbeiter müssen jährlich an einer Schulung zum Thema Sicherheit und Datenschutz teilnehmen. Die Inhalte definieren der Datenschutzbeauftragte (DSB) und der Informationssicherheitsbeauftragte in Abstimmung mit der Geschäftsführung.
Neue Mitarbeiter erhalten im Zuge des HEGENSCHEIDT-MFD Einarbeitungsprogramms eine Schulung, bzw. Erhalten in der Einführungsmappe erste wichtige Informationen.

7.5.2 Spezifische Informationssicherheitsrichtlinien

Diese vorliegende übergreifende Informationssicherheitsleitlinie wird durch diverse themenspezifische Sicherheitsrichtlinien ergänzt und unterstützt. Jeder Mitarbeiter muss diese

Richtlinien anwenden und einhalten, insofern sie für seine Rolle und Position im Unternehmen relevant sind.

7.5.3 Meldung bei Gefährdung oder Verstößen

Meldepflichtig sind alle Ereignisse, die eine Datenschutzverletzung darstellen, oder die Informationssicherheit gefährden könnten.
Jedes (potenzielle) Ereignis muss gemeldet werden. Der Meldeweg sollte der Kritikalität des Ereignisses sowie der zeitlichen Dringlichkeit einer Reaktion entsprechend angemessen gewählt werden.
HEGENSCHEIDT-MFD stellt für Meldungen folgende Möglichkeiten zur Verfügung:
per E-Mail:

datenschutz@nshgroup.com	(Meldungen für Datenschutzereignisse),
isb@nshgroup.com	(Meldungen für Informationssicherheitsereignisse),
j.zohren@nshgroup.com	(Meldungen für IT-Anforderungen und Probleme)

oder

aber die Rufnummer des IT 1st Level Supports 0151 538 86 236 Herr J. Zohren

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

7.6 Rollen und Verantwortlichkeiten

7.6.1 Geschäftsführung

Die Geschäftsführung ist das oberste Organ der Informationssicherheit und des Datenschutzes. Die Geschäftsführung stellt benötigte Ressourcen zur Verfügung und unterstützt die kontinuierliche Verbesserung der Informationssicherheit und des Datenschutzes. Darüber hinaus werden Verantwortlichkeiten strikt voneinander getrennt; so werden Interessenkonflikte vermieden.

7.6.2 Informationssicherheitsbeauftragter

Der Informationssicherheitsbeauftragte wurde von der Geschäftsführung benannt. Diese Rolle stellt sicher, dass das ISMS bei HEGENSCHEIDT-MFD entsprechend der Vorgaben der Geschäftsführung etabliert, betrieben und verbessert wird.

7.6.3 Risikomanager

Die Aufgabe des Risikomanagers wird bei HEGENSCHEIDT-MFD durch den Informationssicherheitsbeauftragten abgebildet. Der Informationssicherheitsbeauftragte wird durch die Fachabteilungen, oder den Verantwortlichen anderer Managementsysteme unterstützt. Der Risikomanager ist für die Planung, Umsetzung, Überwachung und Verbesserung des Risikomanagements gemäß des Risikomanagementprozesses verantwortlich. Risiken des Datenschutzes sind durch den DSB zu bewerten und entsprechende Maßnahmen einzuleiten.

Eine Risiko-Chancen-Bewertung ist mindestens einmal im Jahr durchzuführen. Die Geschäftsführung hat Risikoakzeptanzkriterien festgelegt und ist im Falle einer Überschreitung zwingend einzubinden.

7.6.4 Datenschutzbeauftragter (DSB)

Der DSB wurde von der Geschäftsführung benannt. Der DSB unterstützt die Organisation, den Datenschutz gemäß den gesetzlichen Vorgaben zu gewährleisten.

7.6.5 Asset Owner

Assets (Werte) sind zu schützen. Werte können in unterschiedlicher Form vorliegen (bspw.: Geschäftsprozesse, Informationen, Hard- und Software, IT-Systeme, allgemeine Vermögenswerte, Ansehen und Reputation der HEGENSCHEIDT-MFD). Jedem Wert ist einem Asset Owner zuzuordnen.

7.6.6 Prozessverantwortlicher

Geschäftsprozesse bilden die Grundlage der HEGENSCHEIDT-MFD Geschäftsfähigkeit. Die HEGENSCHEIDT-MFD Geschäftsprozesse werden in Management-, Kern- und Unterstützungsprozesse unterteilt. Der Prozessverantwortliche ist für die Definition der Prozessziele, Kennzahlen und Rahmenbedingungen, für die Bereitstellung der entsprechenden Ressourcen sowie für die Kontrolle der Zielerreichung verantwortlich. Der Prozessverantwortliche überprüft regelmäßig, ob die Prozesse an die sich veränderten Geschäftsanforderungen anzupassen sind.

7.6.7 Mitarbeiter

Jeder Mitarbeiter ist verpflichtet, die Prozesse von HEGENSCHEIDT-MFD zur Aufrechterhaltung der gesetzlichen und normativen Vorgaben zu befolgen. Des Weiteren ist er für die ihm im Rahmen seiner Aufgaben und Projekte, etc. anvertrauten Informationen verantwortlich.

7.7 Kontrolle

Als übergeordnetes Managementsystem wird das ISMS regelmäßig oder anlassbezogen mit Hilfe eines Auditprogramms oder benötigter Risikoanalysen überprüft. Der Informationssicherheitsbeauftragte hat über den Status der Informationssicherheit regelmäßig und direkt an die Geschäftsführung zu berichten.

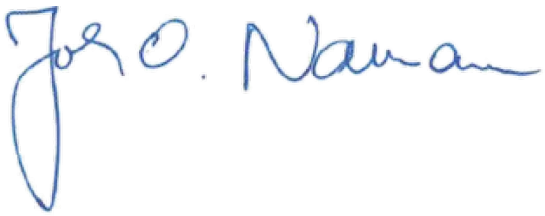
8 Veröffentlichung

Diese Leitlinie wurde am 03.11.2023 von der Geschäftsführung der HEGENSCHEIDT-MFD beschlossen.

Sie ist ab sofort wirksam.

Geprüft: Kasimir, 03.11.2023

Freigabe:



Erkelenz, den 03.11.2023

John Oliver Naumann
HEGENSCHEIDT-MFD GmbH
President & CEO