Qualitätsmanagement Verlag

Seiler Dokumentationen

Informationssicherheitsmanagement

Handbuch

DIN EN ISO 27001:2015

Auflage 1

ISBN: 978-3-942882-67-5

Handbuch / Regelwerk zur Norm
DIN EN ISO 27001:2015

Inhaltsverzeichnis

1 Anwendungsbereich

Unternehmensbezeichnung:	Mustermann AG
Straße:	Zum Salm 27
PLZ, Ort:	D-88662 Überlingen
GF:	Klaus Seiler, MSc. in QM
ISMS-Beauftragte(r):	Hans Mustermann
Anzahl Mitarbeiter/-innen:	5

2 Normative Verweisungen

Im Rahmen unseres Informationsmanagementsystems beachten wir folgende normative Vorgaben (Beispiele):

- DIN ISO / IEC 27000:2011-07 Überblick / Terminologie
- DIN ISO / IEC 27001:2015-03 Anforderungen Informationssicherheitsmanagementsysteme
- DIN ISO / IEC 27002:2014-02 Leitfaden
- DIN ISO / IEC 27003:2010-02 Anleitung zur Umsetzung
- DIN ISO / IEC 27004:2009-12 Messgrößen
- BS ISO / IEC 27005:2011-06 Risikomanagement
- ISO / IEC DIS 27006:2015-01 Anforderungen an Zertifizierungsstellen
- ISO / IEC 27007:2011-11 Auditrichtlinien
- ISO / IEC 27011:2008-12 Telekommunikationsunternehmen
- DIN EN ISO 27799:2014-10 Gesundheitsorganisationen
-

3 Begriffe (siehe Punkt 11)

4 Kontext der Organisation

4 1 Verstehen der Organisation und ihres Kontextes

Unsere Rahmenbedingungen sind für die strategische Ausrichtung unseres Informationssicherheitsmanagementsystems relevant. Die Themen zur Erreichung der beabsichtigten Ergebnisse sind in externe und interne Zusammenhänge unterteilt. Die Themen werden laufend, formell aber jährlich geprüft und überwacht. Werden zwischen den Überwachungen neue Themen erkannt, werden diese umgehend umgesetzt.

Dabei berücksichtigen wir folgende Aspekte:

- soziale, kulturelle, politische, rechtliche, regulatorische, finanzielle, technologische, wirtschaftliche, natürliche und wettbewerbsspezifische Gegebenheiten internationaler, nationaler, regionaler oder lokaler Art,
- wesentliche Triebkräfte und Trends, welche unser Unternehmen beeinflussen,
- die Beziehungen zu interessierten Parteien sowie deren Wahrnehmungen und Werte.

Nachweis(e)
FB 4 1 0 / 4 2 0 Kontext, Erfordernisse und Erwartungen

4 2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien

Wir haben die Erfordernisse und Erwartungen in einem Formblatt gelistet und kommunizieren diese im Unternehmen. Die Erfordernisse und Erwartungen werden laufend, formell aber jährlich geprüft und überwacht. Werden zwischen den Überwachungen neue Erfordernisse und Erwartungen erkannt, werden diese umgehend umgesetzt.

Nachweis(e)
FB 4 1 0 Kontext, Erfordernisse und Erwartungen

4 3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems

Anwendungsbereich des ISMS:

- Entwicklung, Produktion und Vertrieb von Musterdokumentationen,
- Durchführung von Beratungsleistungen,
- Informationsmanagement für Kunden,
- Dokumentationsprüfungen und
- Dokumentationserstellung.

Geografischer Anwendungsbereich:

Siehe 1 Anwendungsbereich.

Nachweis(e)

FB 4 3 0 Grundriss Räumlichkeiten

4 4 Informationssicherheitsmanagementsystem

Mit diesem Handbuch und den nachfolgenden Regelungen und Nachweisen haben wir nachgewiesen, dass wir ein ISMS eingeführt haben. Dieses System wird fortlaufend aufrechterhalten und verbessert.
Unsere Prozesse sind im Laufe dieses Regelwerks oder in gesonderten Prozessbeschreibungen beschrieben.
Die Prozessbeschreibungen beinhalten:

- die Prozesseingaben,
- das zu erwartende Prozessergebnis,
- Kriterien und Methoden zur Durchführung,
- die Art der Messung,
- Messmethoden,
- bedeutende Leistungsindikatoren, die für das Prozessergebnis von Bedeutung sind,
- Verantwortungen / Befugnisse im Rahmen des Prozessablaufes,
- Prozessrisiken und Chancen sowie abgeleitete Maßnahmen,
- die Form der Prozessüberwachung,
- letzte Änderungen,
- mögliche Prozessverbesserungen ,
- Dokumente und deren Aufbewahrung und
- die Prozessabfolge und deren Wechselwirkungen.

Dokumentierte Informationen, wie Aufzeichnungen und Vorgaben, stehen im Einklang mit der Notwendigkeit und unterstützen die Durchführung.

Arbeitsanweisung

AA 4 4 0 Anweisung Prozesserstellung

Nachweis(e)

FB 4 4 0 Prozesse

5 Führung

5 1 Führung und Verpflichtung

5 1 1 Führung und Verpflichtung

Wir zeigen Führung und Verpflichtung durch:

- Festlegung der Informationssicherheitspolitik und der Informationssicherheitsziele unter Beachtung der strategischen Ausrichtung,
- Umsetzung in allen Geschäftsprozessen,
- Bereitstellung von notwendigen Ressourcen,
- Laufende Vermittlung des ISMS auf allen internen Ebenen,
- Gewährleistung der Zielerreichung,
- Unterstützung und Anleitung der Beteiligten,
- Fortlaufende Verbesserung und
- Unterstützung der Führungskräfte.

5 2 Politik

Unsere Informationssicherheitspolitik ist für den Zweck und den Kontext unserer Organisation geeignet. Sie bildet den Rahmen zur Festlegung und Überprüfung der Informationssicherheitsziele. Wir verpflichten uns zur Erfüllung der ermittelten Anforderungen und zur laufenden Verbesserung.

Unsere Informationssicherheitspolitik ist im Formblatt 5.2.0 Informationssicherheitspolitik festgelegt. Sie wurde allen Mitarbeitern/-innen vermittelt und wird angewendet. Die Informationssicherheitspolitik wird den interessierten Parteien zur Verfügung gestellt.

Nachweis(e)

FB 5 2 0 Informationssicherheitspolitik

5 3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation

Die Verantwortlichkeiten und Befugnisse für relevante Rollen sind zugewiesen, intern kommuniziert und werden verstanden.

Wir haben Verantwortungen und Befugnisse zugewiesen für:

- die Sicherstellung, dass das ISMS die Normforderungen erfüllt,
- die Sicherstellung, dass die beabsichtigten Prozessergebnisse geliefert werden,
- eine Berichterstattung über die
  - Leistung,
  - Verbesserungsmöglichkeiten,
  - Änderungen und
  - Innovation des Informationssicherheitsmanagementsystems,
- die Förderung der Kundenorientierung,
- die Aufrechterhaltung der Integrität bei Änderungen des ISMS.

Nachweis(e)

FB 5 3 0 Organisationsdiagramm,
FB 5 3 0 Informationssicherheitsrichtlinien
FB 5 3 0 Lieferantensicherheitsrichtlinie
FB 5 3 0 Verantwortungen und Befugnisse

6 Planung

6 1 Maßnahmen zum Umgang mit Risiken und Chancen

6.1.1 Allgemeines

Aus unseren Themen zum Kontext (4.1) und Anforderungen (4.2) haben wir Risiken und Chancen bestimmt. Sie dienen dazu, die beabsichtigten Ergebnisse zu erzielen, unerwünschte Auswirkungen zu verhindern und zu verringern und eine fortlaufende Verbesserung zu erreichen.

Die Betrachtungen gewährleisten:

- Verringern und verhindern von ungewünschten Auswirkungen,
- Die Sicherstellung zur Erreichung der beabsichtigten Ergebnisse,
- Eine fortlaufende Verbesserung,
- die Planung zum Umgang mit Risiken, Chancen und der Integration von Prozessen sowie der
- Wirksamkeitsbeurteilung.

Prozess(e)

PA 6 1 0 Chancen und Risiken

Nachweis(e)

FB 6 1 0 Chancen und Risiken

6.1.2 Informationssicherheitsrisikobeurteilung

Wir haben einen Prozess zur Informationssicherheitsrisikobeurteilung festlegt und wenden diesen an.

Der Prozess gewährleistet:

- Die Festlegungen von Informationssicherheitsrisikokriterien inklusive
  - Akzeptanzkriterien und
  - Beurteilungskriterien,
- Erneute oder wiederholte Beurteilungen zu konsistenten, vergleichbaren und gültigen Ergebnissen führen,
- Die Identifizierung von Informationssicherheitsrisiken in Bezug auf
  - Verlust der Vertraulichkeit,
  - Integrität und Verfügbarkeit von Informationen,
  - Identifizierung von Risikoeigentümern,
  - Eintrittsfolgen,
  - Die Bewertung der Eintrittswahrscheinlichkeit
  - Bestimmung des Risikoniveaus mit
    - Vergleich der Risiken mit den Risikokriterien und
    - Priorisierung der Risikobehandlung

Prozess(e)

PA 6 1 2 Informationssicherheitsrisikobeurteilung

Nachweis(e)

FB 6 1 2 / 6 1 3 Informationssicherheitsrisiko Beurteilung Behandlung

6.1.3 Informationssicherheitsrisikobehandlung

Informationssicherheitsrisiken werden in allen Ebenen beachtet. Der Prozess 6.1.3 Risikomanagement IT lenkt die Informationssicherheitsrisikobehandlung. Mit der nachgeführten Tabelle „Informationssicherheitsrisiko Beurteilung Behandlung“ werden die Risiken gelenkt.

Wir gewährleisten:

- angemessene Optionen für die Behandlung unter Berücksichtigung der Risikobeurteilung,
- festgelegte Maßnahmen zur Umsetzung der gewählten Optionen,
- die Vergleichbarkeit zu Anhang A der Norm,
- eine Erklärung zur Anwendbarkeit,
- einen Plan für die Informationssicherheitsrisikobehandlung zu formulieren und
- den Risikoeigentümern eine Genehmigung des Plans einzuholen.

Prozess(e)
PA 6 1 3 Informationssicherheitsrisikobehandlung
PA 6 1 3 Risikomanagement IT
Nachweis(e)
FB 6 1 0 Chancen und Risiken,
FB 6 1 2 / 6 1 3 Informationssicherheitsrisiko Beurteilung Behandlung

6 2 Informationssicherheitsziele und Planung zu deren Erreichung

Wir haben Informationssicherheitsziele für alle relevanten Funktionen und Ebenen festgelegt.

Wir gewährleisten:

- den Einklang mit der Informationssicherheitspolitik,
- die Messbarkeit,
- anwendbare Informationssicherheitsanforderungen,
- die Ergebnisse der Risikobeurteilung und Risikobehandlung,
- die Vermittlung und
- die Aktualität.

In der Planung der Qualitätsziele (siehe FB 6 2 0 Qualitätsziele) haben wir folgende Fragestellungen geregelt:

- Was wird getan?
- Welche Ressourcen sind erforderlich?
- Wer ist verantwortlich?
- Wann ist das Ziel abgeschlossen?
- Wie werden Ergebnisse bewertet?

Prozess(e)
PA 6 2 0 Informationssicherheitsziele
PA 6 2 0 Planung Änderungen
Nachweis(e)
FB 6 2 0 Informationssicherheitsziele

7 Unterstützung

7 1 Ressourcen

Wir haben die Ressourcen für den Aufbau, der Verwirklichung, Aufrechterhaltung und Verbesserung festgelegt und bereitgestellt. Dabei haben wir die Fähigkeiten und Beschränkungen von bestehenden internen Ressourcen und die von externen Anbietern einzuholenden Informationen beachtet.

Nachweis(e)
FB 7 1 0 Werte

7 2 Kompetenz

Wir haben die für die Erbringung unserer Produkte und Dienstleistungen notwendigen Kompetenzen ermittelt. Die Ermittlung betrifft alle Mitarbeiter/-innen, welche die Informationssicherheit beeinflussen können.

Im Formblatt 7 2 0 Kompetenzen lenken wir folgende Fragestellungen:

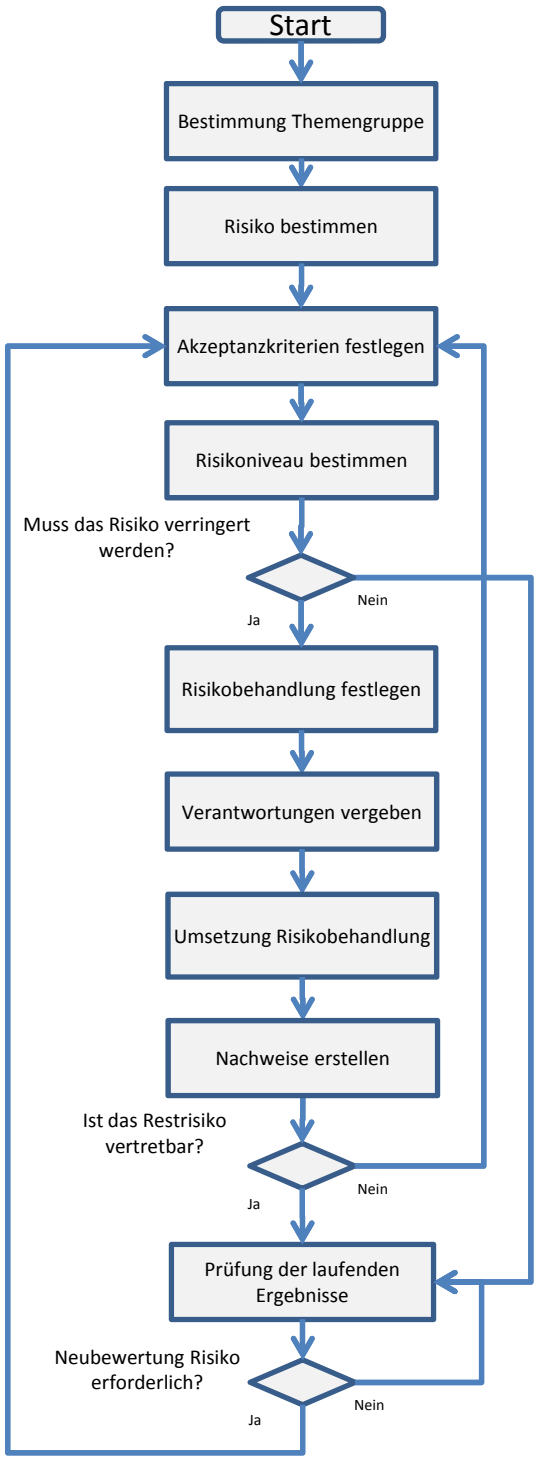
- Kompetenz durch angemessene Ausbildung, Schulung oder Erfahrung,
- Maßnahmen, um die benötigte Kompetenz zu erwerben inkl. deren Bewertung und
- dokumentierte Informationen als Nachweis der Kompetenz aufbewahren.

Mögliche Optionen, um Kompetenzen zu erreichen sind Schulungen, Coaching, Versetzung, Anstellung oder Beauftragung von externen Anbietern auf die, die Anforderungen auch zutreffen.

Prozess(e)
PA 7 2 0 Schulungen, **PA 7 2 0 Erforderliche Kompetenzen**

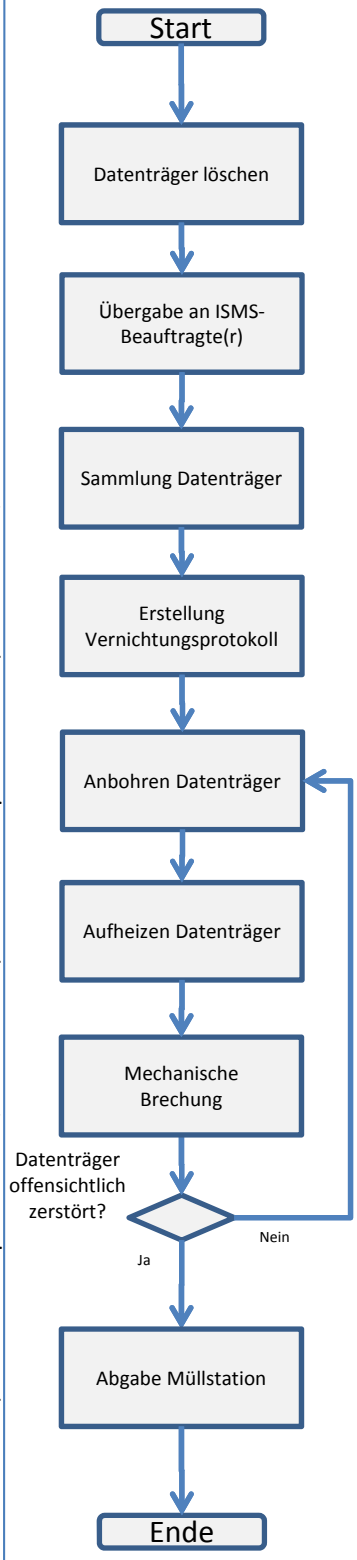
6.1.3 Risikomanagement IT

MA	VA	Ablauf / Tätigkeiten	Dokument	Ablauf / Hilfsmittel
	GF	Bestimmung Themengruppe	DIN ISO IEC 27001:2015	Entsprechend Anhang A
ISMS-Beauftr.	GF	Risiko bestimmen	FB 6.1.2 6.1.3 Informationssicher-heitsrisiko Beurteilung Behandlung	Bestimmung des Risikos
ISMS-Beauftr.	GF	Akzeptanzkriterien festlegen	FB 6.1.2 6.1.3 Informationssicher-heitsrisiko Beurteilung Behandlung	Kriterien für die Akzeptanz des Risikos festlegen
ISMS-Beauftr.	GF	Risikoniveau bestimmen		Bestimmung des Risikoniveaus durch Bewertung des Auftretens, der Bedeutung und der Wahrscheinlichkeit der Entdeckung.
ISMS-Beauftr.	GF	Muss das Risiko verringert werden?	FB 6.1.2 6.1.3 Informationssicher-heitsrisiko Beurteilung Behandlung	Das Risiko muss verringert werden wenn die Akzeptanzkriterien nicht erreicht sind im aktuellen Status
ISMS-Beauftr.	GF	Risikobehandlung festlegen		Festlegung der Maßnahmen zur Beseitigung des Risikos.
ISMS-Beauftr.	GF	Verantwortungen vergeben	FB 6.1.2 6.1.3 Informationssicher-heitsrisiko Beurteilung Behandlung	
ISMS-Beauftr.	GF	Umsetzung Risikobehandlung	Alle Dokumente	Handlungen zur Risikominimierung werden umgesetzt.
ISMS-Beauftr.	GF	Nachweise erstellen	Alle Dokumente	Führen der geeigneten Nachweise
ISMS-Beauftr.	GF	Ist das Restrisiko vertretbar?	FB 6.1.2 6.1.3 Informationssicher-heitsrisiko Beurteilung Behandlung	Das Restrisiko ist vertretbar wenn die Akzeptanzkriterien eingehalten werden.
ISMS-Beauftr.	GF	Prüfung der laufenden Ergebnisse	Alle Dokumente	Laufende Auswertung von Ergebnissen und ständige Neubewertung aller erkannten Risiken
ISMS-Beauftr.	GF	Neubewertung Risiko erforderlich?		Bei abweichenden Ergebnissen oder Vorfällen



8.3.0 Entsorgung Datenträger

MA	VA	Ablauf / Tätigkeiten	Dokumente	Ablauf Hilfsmittel
ISMS-Beauftr.	MA	Datenträger löschen	Liste Werte	Die Daten auf dem Datenträger werden konventionell gelöscht und mehrfach (drei mal) wiederholt. Das Speichermedium wird ausgebaut.
ISMS-Beauftr.	MA	Übergabe an ISMS-Beauftragte(r)	Liste Werte	Bei der Übergabe werden ggfs. weitere Informationen abgegeben wie frühere Verwendung…
MA	ISMS-Beauftr.	Sammlung Datenträger	Liste Werte	Weitere Sammlung von veralteten Datenträgern. Lagerung im Safe bis 10 Stück erreicht sind.
MA	ISMS-Beauftr.	Erstellung Vernichtungsprotokoll	Liste Werte, Vernichtungsprotokoll	Im Protokoll werden alle Seriennummern gelistet. Die Produkte werden aus der Liste Werte gestrichen.
MA	ISMS-Beauftr.	Anbohren Datenträger	Vernichtungsprotokoll	Jeder Datenträger wird drei mal durchbohrt mittels eines Bohrmaschine.
MA	ISMS-Beauftr.	Aufheizen Datenträger	Vernichtungsprotokoll	Jeder Datenträger wird mit einem Heißluftföhn eine Minute auf maximaler Stufe aufgeheizt.
MA	ISMS-Beauftr.	Mechanische Brechung	Vernichtungsprotokoll	Jeder Datenträger wird mittels Hammerschlag erheblich deformiert
MA	ISMS-Beauftr.	Datenträger offensichtlich zerstört? (Nein / Ja)	Vernichtungsprotokoll	Offensichtlich heißt die Anschlüsse sind defekt, das Gehäuse deformiert. Die Löcher durch das Medium getrieben und Schmauchspuren sind vorhanden.
MA	ISMS-Beauftr.	Abgabe Müllstation	Vernichtungsprotokoll	Die Hardware wird in den Elektronikschrott geworfen und das Vernichtungsprotokoll wird abgeschlossen.



8.3.0 Verwendung von Werten außerhalb des Unternehmens

Grundlagen

Kapitel 8 Abschnitt 8.3.0 "ISMS und dessen Prozesse“.

Gültigkeit

Diese Anweisung betrifft alle Personen, die Werte außerhalb des Unternehmens verwenden.

Ziel und Grund

Die Vereinheitlichung der Prozessbeschreibungen im Unternehmen und die Sicherstellung der richtigen Inhalte.

Abkürzungen

GF	Geschäftsführung
QM	Qualitätsmanager/-in
ISMS-Beauftr.	Informationsmanagementsystem-Beauftragte(r)

Zu beachtende Punkte

1. Geräte, Betriebsmittel und Werte außerhalb der Räumlichkeiten werden immer geschützt mittels:
    a. Verschluss
    b. Verbleib in geschlossenen Räumen ohne Aufsicht
    c. Passwort
2. Der Verbleib in Fahrzeugen ist untersagt.
3. Werte werden immer verpackt:
    a. Computertaschen,
    b. Umschläge,
    c. Taschen
4. Bei allen Werten gibt es Informationen zu unserem Unternehmen und der Aufforderung einer Abgabe bei Verlust.
5. Das Autoabschalten bei digitalen Geräten (PDA’s, Lapotop, Notebook…) ist auf den kürzesten Zeitraum einzustellen.
6. Bei dem Gang auf Toiletten, Duschen usw. werden elektronische Werte immer abgeschaltet.
7. Notizen, Anweisungen und Vorgaben werden immer verschlossen.
8. Geheim eingestufte Werte werden nur nach schriftlicher Genehmigung verwendet.
9. Abweichungen werden sofort der / dem ISMS-Beauftragte(n) gemeldet.

5.3.0 Verantwortungen und Befugnisse

Beispiele in Rot

Normforderung	Bereich	Verantwortung	Befugnis
4 Kontext der Organisation	GF	Beschreibung, Prozessfestlegung, Anwendungsbereich festlegen, Erfordernisse und Erwartungen ermitteln	Alle Befugnisse
5 Führung	GF	Verpflichtung festlegen, Kundenorientierung beschreiben, Qualitätspolitik festlegen, Verantwortungen und Befugnisse bestimmen	Alle Befugnisse
6.1 Maßnahmen zum Umgang mit Risiken und Chancen	GF und Informationssicherheitsbeauftragte Alle Bereiche	Maßnahmen zum Umgang mit Risiken und Chancen bestimmen, Informationssicherheitsziele erstellen und deren Erreichung planen, Änderungen planen und umsetzen.	Alle Befugnisse Alle Bereiche Mitarbeit.
6 1 2 Informationssicherheitsrisikobeurteilung	GF und Informationssicherheitsbeauftragte Alle Bereiche	Beurteilung der Informationssicherheitsrisiken und deren Eintrittswahrscheinlichkeit anhand des festgelegten Prozesses. Festlegung von Akzeptanz- und Sicherheitsrisikokriterien. Bestimmung der Risikoeigentümer.	Alle Befugnisse Alle Bereiche Mitarbeit.
6 1 3 Informationssicherheitsrisikobehandlung	GF und Informationssicherheitsbeauftragte Alle Bereiche	Auswahl von Optionen zur Informationssicherheitsrisikobehandlung, Festlegung von Maßnahmen, Begründung von Maßnahmen, Planerstellung zu Informationssicherheitsrisikobehandlung, Genehmigungen bei den Risikoeigentümern einholen.	Alle Befugnisse Alle Bereiche Mitarbeit.
6 2 0 Informationssicherheitsziele	GF und Informationssicherheitsbeauftragte Alle Bereiche	Festlegung der Informationssicherheitsziele und deren Überwachung	Alle Befugnisse Alle Bereiche Mitarbeit.
7 1 Ressourcen	GF Alle Bereiche	Erhebung notwendiger Informationen und Beschaffung von Ressourcen.	Ermittlung und Beschaffung. Informationen erheben.
7 2 Kompetenz	GF und Informationssicherheitsbeauftragte	Ermittlung, Vermittlung von ISMS-Anforderungen.	Alle Befugnisse Durchführung im eigenen Bereich.
7 3 Bewusstsein	Informationssicherheitsbeauftragte	Bewusstseinsförderung zur Wirksamkeit der Informationssicherheitspolitik und den Folgen einer Nichterfüllung	Schulungen, Gespräche, Aushang und Handouts.
7 4 Kommunikation	GF Informationssicherheitsbeauftragte Alle Bereiche	Umfang ermitteln, Inhalte festlegen, Durchführung. Interne und externe Kommunikation.	Alle Befugnisse Durchführung übergeordnet und extern. Durchführung im eigenen Bereich.
7 5 Dokumentierte Information	GF und Informationssicherheitsbeauftragte Alle Bereiche	Umfang prüfen und freigeben; Lenkung, Verwendung	Alle Befugnisse Umfang erstellen, prüfen und freigeben. Aufzeichnungen führen und lenken.
7 5 2 Erstellen und Aktualisieren	Informationssicherheitsbeauftragte Alle Bereiche	Lenkung Vorschläge, fachliche Prüfung	Erstellung und Freigabe. Prüfung, Einspruch und Verwendung.
7 5 3 Lenkung dokumentierter Information	Informationssicherheitsbeauftragte Alle Bereiche	Aufbewahrung	Aufbewahrung festlegen, Prüfung der Aktualität. Aufbewahrung im eigenen Bereich und Datensicherung.

5.3.0 Verantwortungen und Befugnisse

Beispiele in Rot

Normforderung	Bereich	Verantwortung	Befugnis
8 1 Betriebliche Planung und Steuerung	GF Informationssicherheitsbeauftragte	Prozesse planen und deren Aufrechterhaltung Steuerung ausgegliederter Prozesse Überwachung von Änderungen	Alle Befugnisse
8 2 Informationssicherheitsrisikobeurteilung	Informationssicherheitsbeauftragte	Laufende Informationssicherheitsrisikobeurteilung oder bei besonderen Anlässen	Laufende Beurteilung und Vorschlag von Maßnahmen
8 3 Informationssicherheitsrisikobehandlung	Informationssicherheitsbeauftragte	Umsetzung des Plans zur Informationssicherheitsbehandlung	Alle Befugnisse die im Rahmen der Steuerung notwendig sind.
8 4 Kontrolle von extern bereitgestellten Produkten und Dienstleistungen	Einkauf	Lenkung bereitgestellter Produkte und Dienstleistungen	Alle Aufgaben im Rahmen der Beschaffung und der Kontrolle der Leistungsverbesserung.
9 1 Überwachung, Messung, Analyse und Bewertung	Alle Bereiche	Überwachung, Messung, Analyse und Bewertung der Informationssicherheitsleistung	Alle Befugnisse zur Durchführung intern und extern.
9 2 Internes Audit	Auditteam GF Informationssicherheitsbeauftragte	Durchführung Festlegung / Korrekturen	Alle Befugnisse zur Durchführung des Audits. Anordnung zur Durchführung und Bestimmung / Freigabe von Korrekturmaßnahmen
9 3 Managementbewertung	GF Informationssicherheitsbeauftragte Alle Bereiche	Durchführung Vorbereitung Erhebung	Alle Befugnisse. Datenerhebungen in allen Bereichen, Vorbereitung der Bewertung. Erheben von allen Informationen zur Managementbewertung.
10 1 Nichtkonformität und Korrekturmaßnahmen	GF Alle Bereiche Informationssicherheitsbeauftragte	Überwachung und Steuerung Steuerung	Alle Befugnisse Erhebung, Analyse, Maßnahmenfestlegung, Durchführung und Überwachung.
10 2 Fortlaufende Verbesserung	GF / Informationssicherheitsbeauftragte	Steuerung / Überwachung / Durchführung	Alle Befugnisse

managementsysteme Seiler; Zum Salm 27; 88662 Überlingen / See

Anrede

Name

Straße

D-PLZ Ort

Ort, den

Benennung zum / zur ISMS-Beauftragte(n)

Ihre Aufgaben:

- Fortlaufende Ermittlung von:
  - Anforderungen der Kunden,
  - Gesetzliche Anforderungen,
  - Behördliche Anforderungen und
  - Regulatorischen Anforderungen.
- Sicherstellung der wirksamen Durchführung des ISMS,
- Überwachung der getroffenen Regelungen,
- Unterstützung der Abteilungen,
- Weisungsbefugnis in Themen der Datensicherheit gegenüber allen Personen im Unternehmen,
- Ermittlung und Festlegung benötigter Prozesse.

Weitere Verantwortungen sind im ISMS hinterlegt.

Ort, xx.xx.xxxx

_____ _____

GF Qualitätsmanager/-in

Qualitätsmanagement Verlag

Seiler Dokumentation

7.5.1 Dokumentierte Informationen

Dokumentenübersicht	Revision	vom	Ersteller/-in	Verteiler	Grund der letzten Änderung
Handbuch					
Handbuch gesamt mit Kapitel 1 bis 10	0		QM	QM	
Prozessbeschreibungen / Verfahren					
6 1 0 Ermittlung Risiken Chancen	0		QM	QM	
6 1 2 Informationssicherheitsrisikobeurteilung	0		QM	QM	
6 1 3 Informationssicherheitsbehandlung	0		QM	QM	
6 1 3 Risikomanagement IT	0		QM	QM	
6 2 0 Informationssicherheitsziele	0		QM	QM	
6 3 0 Planung Änderungen	0		QM	QM	
7 2 0 Erforderliche Kompetenzen	0		QM	QM	
7 2 0 Schulungen	0		QM	QM	
7 2 0 Weiterbildung	0		QM	QM	
7 4 0 Externe Kommunikation	0		QM	QM	
7 4 0 Interne Kommunikation	0		QM	QM	
7 5 3 Lenkung aufgezeichneter Informationen	0		QM	QM	
7 5 3 Lenkung externer Informationen	0		QM	QM	
7 5 3 Lenkung interner Informationen	0		QM	QM	
8 3 0 Änderungen am System	0		QM	QM	
8 3 0 Auswahl Anbieter	0		QM	QM	
8 3 0 Benutzerzugang	0		QM	QM	
8 3 0 Berechtigung	0		QM	QM	
8 3 0 Beschaffung	0		QM	QM	
8 3 0 Eigentum Kunden Anbieter	0		QM	QM	
8 3 0 Entsorgung Datenträger	0		QM	QM	
8 3 0 Entwicklungsänderungen	0		QM	QM	
8 3 0 Entwicklungsbewertung	0		QM	QM	
8 3 0 Entwicklungseingaben	0		QM	QM	
8 3 0 Entwicklungsergebnisse	0		QM	QM	

7.5.1 Dokumentierte Informationen

Dokumentenübersicht	Revision	vom	Ersteller/-in	Verteiler	Grund der letzten Änderung
8 3 0 Entwicklungsplanung	0		QM	QM	
8 3 0 Entwicklungsvalidierung	0		QM	QM	
8 3 0 Entwicklungsverifizierung	0		QM	QM	
8 3 0 Externe Wartungen	0		QM	QM	
8 3 0 Genehmigung neuer Einrichtungen	0		QM	QM	
8 3 0 Informationsübertragung	0		QM	QM	
8 3 0 Informationen	0		QM	QM	
8 3 0 Installation	0		QM	QM	
8 3 0 Interne Wartung	0		QM	QM	
8 3 0 Kennzeichnung und Rückverfolgbarkeit	0		QM	QM	
8 3 0 Kennzeichnung von Informationen	0		QM	QM	
8 3 0 Kommunikation Anbieter	0		QM	QM	
8 3 0 Kontrolle Lieferungen	0		QM	QM	
8 3 0 Lieferanten / Anbieteraudit	0		QM	QM	
8 3 0 Notfallvorsoge Management	0		QM	QM	
8 3 0 Registrierung / Deregistrierung	0		QM	QM	
8 3 0 Sammlung Beweismaterial	0		QM	QM	
8 3 0 Sicherheitsvorfall	0		QM	QM	
8 3 0 Validierung Software	0		QM	QM	
8 3 0 Wechselmedien	0		QM	QM	
9 1 0 Leistung Anbieter	0		QM	QM	
9 1 0 Leistungsanalyse	0		QM	QM	
9 2 0 Internes Audit	0		QM	QM	
10 1 0 Nichtkonformitäten Dienstleistung	0		QM	QM	
10 1 0 Nichtkonformitäten Produkt	0		QM	QM	
10 2 0 Planung Verbesserung	0		QM	QM	
Arbeitsanweisungen					
4 4 0 Anweisung Prozesserstellung	0		QM	QM	
8 3 0 Arbeiten in Sicherheitsbereichen	0		QM	QM	

Qualitätsmanagement Verlag

Seiler Dokumentation

7.5.1 Dokumentierte Informationen

Dokumentenübersicht	Revision	vom	Ersteller/-in	Verteiler	Grund der letzten Änderung
8 3 0 Entwicklungssteuerung	0		QM	QM	
8 3 0 Kennzeichnung Informationen	0		QM	QM	
8 3 0 Kontrolle Bereitstellungen	0		QM	QM	
8 3 0 Transaktionen bei Anwendungsdiensten	0		QM	QM	
8 3 0 Verwendung von Werten außerhalb des Unternehmens	0		QM	QM	
Formblätter / Nachweisformen					
4 1 0 Kontext, Erfordernisse und Erwartungen	0		QM	QM	
4 4 0 Grundriss Räumlichkeiten	0		QM	QM	
4 4 0 Prozesse	0		QM	QM	
5 2 0 Informationssicherheitspolitik	0		QM	QM	
5 2 0 Informationssicherheitsrichtlinie	0		QM	QM	
5 2 0 Lieferantensicherheitsrichtlinie	0		QM	QM	
5 3 0 Organisationsdiagramm	0		QM	QM	
5 3 0 Verantwortungen und Befugnisse	0		QM	QM	
6 1 0 Chancen und Risiken	0		QM	QM	
7 1 0 Werte	0		QM	QM	
7 2 0 Benennung ISMS Beauftragte	0		QM	QM	
7 2 0 Kompetenzen	0		QM	QM	
7 2 0 Schulungsplan	0		QM	QM	
7 4 0 Liste Kommunikationswege	0		QM	QM	
7 4 0 Protokoll Besprechung	0		QM	QM	
7 5 1 Dokumentierte Informationen (diese Liste)	0		QM	QM	
8 1 0 Planung und Steuerung	0		QM	QM	
8 2 0 Informationssicherheitsbeurteilung	0		QM	QM	
8 3 0 Abnahmetest Software	0		QM	QM	
8 3 0 Änderungssteuerung	0		QM	QM	
8 3 0 Aktionsplan baulich organisatorisch	0		QM	QM	
8 3 0 Ausgabe Mobilgeräte	0		QM	QM	
8 3 0 Ausgabeliste Schlüssel	0		QM	QM	

7.5.1 Dokumentierte Informationen

Dokumentenübersicht	Revision	vom	Ersteller/-in	Verteiler	Grund der letzten Änderung
8 3 0 Berechtigungen	0		QM	QM	
8 3 0 Entsorgungsprotokoll Wiederverwendung	0		QM	QM	
8 3 0 Entwicklungsänderungen	0		QM	QM	
8 3 0 Geheime Authentifizierungsinformationen	0		QM	QM	
8 3 0 Information Arbeitsumgebung	0		QM	QM	
8 3 0 Infrastruktur Netzwerkplan	0		QM	QM	
8 3 0 Kapazitätssteuerung	0		QM	QM	
8 3 0 Kennwortsystem	0		QM	QM	
8 3 0 Kennzeichnung / Rückverfolgung	0		QM	QM	
8 3 0 Konfiguration Medien	0		QM	QM	
8 3 0 Liste Anbieter	0		QM	QM	
8 3 0 Liste bindende Vorgaben	0		QM	QM	
8 3 0 Liste der Berechtigungen	0		QM	QM	
8 3 0 Maßnahmen Wartung	0		QM	QM	
8 3 0 Notfallplan	0		QM	QM	
8 3 0 Protokollierung Überwachung	0		QM	QM	
8 3 0 Prüfplan	0		QM	QM	
8 3 0 QSV Qualitätssicherungsvereinbarung	0		QM	QM	
8 3 0 Regelwerk Zugangskontrolle	0		QM	QM	
8 3 0 Schweigepflicht externe Anbieter	0		QM	QM	
8 3 0 Schweigepflicht Verantwortungsbelehrung	0		QM	QM	
8 3 0 Sicherheitseinstufungen	0		QM	QM	
8 3 0 Tätigkeiten Installation	0		QM	QM	
8 3 0 Überwachung Änderungen	0		QM	QM	
8 3 0 Unterschriftenliste	0		QM	QM	
8 3 0 Zugangssteuerung	0		QM	QM	
9 1 0 Informationssicherheitsbericht	0		QM	QM	
9 1 0 Leistung Anbieter	0		QM	QM	
9 1 0 Leistungsbewertung	0		QM	QM	
9 2 0 Auditbericht	0		QM	QM	

7.5.1 Dokumentierte Informationen

Dokumentenübersicht	Revision	vom	Ersteller/-in	Verteiler	Grund der letzten Änderung
9 2 0 Auditcheckliste 27001 2015	0		QM	QM	
9 2 0 Auditplan	0		QM	QM	
9 2 0 Auditprogramm	0		QM	QM	
9 3 0 Managementbewertung	0		QM	QM	
10 1 0 Fehlerliste	0		QM	QM	
10 1 0 Maßnahmenplan	0		QM	QM	
10 1 0 8 D Report	0		QM	QM	
10 2 0 Liste Verbesserungen	0		QM	QM	

Liste geprüft und freigegeben:

Datum: Funktion, Unterschrift

8.3.0 Sicherheitseinstufungen

Beispiele in Rot

Folgende Sicherheitseinstufungen werden in unserem Unternehmen angewandt. Sie treffen für Dokumente, Personen und Einrichtungen zu.

Öffentlich	Alle Dokumente, die keinerlei Sicherheitsrisiko bieten, wenn sie der Öffentlichkeit zugänglich gemacht werden oder in die Öffentlichkeit geraten. Bearbeiten und Entfernen der Daten ist problemlos möglich.
Minimale Vertraulichkeit	Alle Dokumente, die minimale Vertraulichkeit erfordern. Sie beinhalten kundenbezogene Daten wie z.B. Lieferscheine. Der Umgang mit diesen Dokumenten ist nur zweckmäßig anzuwenden.
Vertraulich	Alle Dokumente, die vertraulich behandelt werden sollten wie z.B. Rechnung. Die Herausgabe und Änderung dieser Dokumente sollte nur bestimmten Personen genehmigt werden.
Streng vertraulich	Streng vertrauliche Dokumente dürfen keinesfalls außer Haus gebracht werden. Die Bearbeitung dieser ist nur einem engen Personenkreis gestattet.
Höchste Geheimhaltung	Höchste Geheimhaltungsstufe

Auflistung der Dokumente:

Öffentlich	Lieferscheine
Minimale Vertraulichkeit	Rechnungen
Vertraulich	…
Streng vertraulich	….
Höchste Geheimhaltung	Bankdaten