6.1.2 Risikobewertung der Informationssicherheit

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 auf der Grundlage von Kriterien 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 Behandlung von Informationssicherheitsrisiken

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 mit
  - erforderlichen Maßnahmen,
  - den Gründen für die Einbeziehung,
  - den Grad der Umsetzung und
  - Gründe für die Nichteinbeziehung
- 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
FB 6 1 3 Relevante Risiken

6 2 Informationssicherheitsziele und Planung zu deren Erreichung

Wir haben Informationssicherheitsziele für alle relevanten Funktionen und Ebenen festgelegt.
Wir gewährleisten:

- den Einklang mit der Informationssicherheitsrichtlinie,
- 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

6.3 Planung von Änderungen

Wenn wir die Notwendigkeit von Änderungen am Informationssicherheits-Managementsystem feststellen, werden diese geplant durchgeführt.

7 Unterstützung

7 1 Ressourcen

Wir haben die notwendigen Ressourcen für den Aufbau, der Verwirklichung, Aufrechterhaltung und Verbesserung festgelegt und bereitgestellt.
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
PA 7 2 0 Weiterbildung,
Nachweis(e)
FB 7 2 0 Kompetenzen

7 3 Bewusstsein

Alle Mitarbeiter/-innen und Externe werden zur Bewusstseinsförderung informiert über:

- die Informationssicherheitsrichtlinie,
- relevante Informationssicherheitsziele,
- ihren Beitrag zur Wirksamkeit des Informationssicherheitssystems,
- der Vorteile einer verbesserten Informationssicherheitsleistung und
- der Folgen von Nichterfüllung der Anforderungen.

Dies geschieht mittels Schulungen und / oder Aushang.

7 4 Kommunikation

Wir haben eine Liste der Kommunikationswege erstellt. Darin wird die externe und interne Kommunikation beschrieben.
Dabei beachten wir mindestens die folgenden vier Punkte:

- Was wird kommuniziert?
- Wann wird kommuniziert?
- Mit wem wird kommuniziert?
- Wie wird kommuniziert?

Prozess(e)
PA 7 4 0 Interne Kommunikation,
PA 7 4 0 Externe Kommunikation
Nachweis(e)
FB 7 4 0 Protokoll Besprechung,
FB 7 4 0 Liste Kommunikationswege

7 5 Dokumentierte Information

7 5 1 Allgemeines

Unsere Dokumentation zum Qualitätsmanagementsystem beinhaltet:

- alle geforderten Informationen der ISO IEC 27001,
- ein Handbuch als Rahmen für das Informationssicherheitsmanagementsystem,
- Prozessbeschreibungen, Arbeitsanweisungen und Nachweise sowie
- weitere Informationen.

Alle festgelegten und angewendeten Informationen sind in einer Liste aufgeführt. Der Umfang ist für unser Unternehmen angemessen.

Nachweis(e)

FB 7 5 1 Dokumentierte Informationen

7 5 2 Erstellen und Aktualisieren

Unsere dokumentierten Informationen beinhalten immer:

- Eine Kennzeichnung und Beschreibung mit:
  - Titel,
  - Datum,
  - Copyrighthinweis und
  - Referenznummer (Ursprung in der Norm)
- angemessene Format, das folgendes berücksichtigt:
  - Sprache,
  - Softwareversion,
  - Graphiken und
  - Elektronische Medien oder Papier an Arbeitsplätzen ohne elektronischen Zugang.
- Überprüfung und Genehmigung durch festgelegte Kompetenzinhaber im Hinblick auf Eignung und Angemessenheit.
- Den Verweis zur Einstufung bei geheimen Dokumenten.
- Der Autor geht jeweils aus der Liste der dokumentierten Informationen hervor.

7 5 3 Lenkung dokumentierter Informationen

Dokumentierte Informationen werden an den vorgesehenen Verwendungsorten bereitgestellt. Dabei ist auf eine Verwendungsmöglichkeit geachtet.

Alle dokumentierten Informationen werden angemessen geschützt in Bezug auf:

- Verlust,
- Vertraulichkeit,
- unsachgemäßem Gebrauch und
- Verlust der Integrität.

Bei der Lenkung dokumentierter Informationen beachten wir:

- die Verteilung,
- den Zugriff mit Berechtigungen,
- die Auffindbarkeit und Verwendung,
- die Ablage/Speicherung und Erhaltung,
- die Aufrechterhaltung der Lesbarkeit,
- die Überwachung von Änderungen und Versionierungen,
- Aufbewahrung und Verfügung bis zur Vernichtung.

Dokumentierte Informationen externer Herkunft werden zentral verwaltet und im Intranet nach Scan den Anwendern/-innen zur Verfügung gestellt.

Prozess(e)

PA 7 5 3 Lenkung externer Informationen,
PA 7 5 3 Lenkung interner Informationen,
PA 7 5 3 Lenkung aufgezeichneter Informationen

8 Betrieb

8 1 Operative Planung und Steuerung

Anforderungen an unser Sicherheitsmanagementsystem sind im Formblatt „6.1.2./ 6.1.3 Informationssicherheitsrisiko Beurteilung Behandlung“ beschrieben.
Für unsere Prozesse sind Kriterien festgelegt die kontrolliert werden. Extern realisierte Prozesse werden kontrolliert.
Wir haben alle notwendigen dokumentierten Informationen im notwendigen Umfang erstellt und erhalten diese aufrecht. Änderungen werden überwacht und dokumentiert. Dabei werden die mögliche Auswirkungen stets beachtet und minimiert.

Nachweis(e)

FB 8 1 0 Planung und Steuerung

8 2 Risikobewertung der Informationssicherheit

Unter Beachtung der Kriterien zu Informationssicherheitsrisiken (siehe 6.1.2 und 6.1.3), beurteilen wir alle drei Monate oder bei besonderen Anlässen das Informationssicherheitsrisiko. Die Ergebnisse werden im Formblatt Informationssicherheitsbericht dokumentiert.

Nachweis(e)

FB 6 1 2 6 1 3 Informationssicherheitsrisiko Beurteilung Behandlung
FB 8 3 0 Behandlungsplan Informationssicherheitsrisiken
FB 9 1 0 Informationssicherheitsbericht

8 3 Umgang mit Informationssicherheitsrisiken

Im Rahmen der Informationsrisikobehandlung haben wir vielfältige dokumentierte Informationen erstellt (siehe Nachweise). Der Plan zur Risikobehandlung erstreckt sich somit über mehrere dokumentierte Informationen.

Prozess(e)

PA 8 3 0 Änderungen am System
PA 8 3 0 Auswahl Anbieter
PA 8 3 0 Benutzerzugang
PA 8 3 0 Berechtigung
PA 8 3 0 Beschaffung
PA 8 3 0 Eigentum Kunden Anbieter
PA 8 3 0 Entsorgung Datenträger
PA 8 3 0 Entwicklungsänderungen
PA 8 3 0 Entwicklungsbewertung
PA 8 3 0 Entwicklungseingaben
PA 8 3 0 Entwicklungsergebnisse
PA 8 3 0 Entwicklungsplanung
PA 8 3 0 Entwicklungsvalidierung
PA 8 3 0 Entwicklungsverifizierung
PA 8 3 0 Externe Wartungen
PA 8 3 0 Genehmigung neuer Einrichtungen
PA 8 3 0 Informationsübertragung
PA 8 3 0 Informationen
PA 8 3 0 Installation
PA 8 3 0 Interne Wartungen
PA 8 3 0 Kennzeichnung von Informationen
PA 8 3 0 Kennzeichnung Rückverfolgung
PA 8 3 0 Kommunikation Anbieter
PA 8 3 0 Kontrolle Lieferungen
PA 8 3 0 Lieferanten Anbieteraudit
PA 8 3 0 Notfallvorsorge Management
PA 8 3 0 Sammlung Beweismittel
PA 8 3 0 Sicherheitsvorfall
PA 8 3 0 Registrierung Deregistrierung
PA 8 3 0 Wechselmedien

Arbeitsanweisung(en)

AA 8 3 0 Arbeiten in Sicherheitsbereichen
AA 8 3 0 Entwicklungssteuerung
AA 8 3 0 Kennzeichnung Informationen
AA 8 3 0 Kontrolle Bereitstellungen
AA 8 3 0 Transaktionen bei Anwendungsdiensten
AA 8 3 0 Validierung Software
AA 8 3 0 Verwendung von Werten außerhalb des Unternehmens

Nachweis(e)

FB 8 1 0 Planung und Steuerung
FB 8 2 0 Informationssicherheitsbeurteilung
FB 8 3 0 Abnahmetest Software
FB 8 3 0 Änderungssteuerung
FB 8 3 0 Aktionsplan baulich organisatorisch
FB 8 3 0 Ausgabe Mobilgeräte
FB 8 3 0 Ausgabeliste Schlüssel
FB 8 3 0 Behandlung ISMS Risiken
FB 8 3 0 Berechtigungen
FB 8 3 0 Entsorgungsprotokoll Wiederverwendung
FB 8 3 0 Entwicklungsänderungen
FB 8 3 0 Infrastruktur netzwerkplan
FB 8 3 0 Kapazitätssteuerung
FB 8 3 0 Kennwortsystem
FB 8 3 0 Kennzeichnung Rückverfolgung
FB 8 3 0 Konfiguration Medien
FB 8 3 0 Liste Anbieter
FB 8 3 0 Liste bindende Vorgaben
FB 8 3 0 Liste der Berechtigungen
FB 8 3 0 Liste externe Betriebsmittel
FB 8 3 0 Maßnahmen Wartung
FB 8 3 0 Notfallplan
FB 8 3 0 Protokollierung Überwachung
FB 8 3 0 Prüfplan
FB 8 3 0 QSV
FB 8 3 0 Regelwerk Zugangskontrolle
FB 8 3 0 Schlüsselverwaltung
FB 8 3 0 Schweigepflicht externe Anbieter
FB 8 3 0 Schweigepflicht Verantwortungsbelehrung
FB 8 3 0 Sicherheitseinstufungen
FB 8 3 0 Tätigkeiten Installation
FB 8 3 0 Überwachung Änderungen
FB 8 3 0 Unterschriftenliste
FB 8 3 0 Zugangssteuerung

9 Bewertung der Leistung

9 1 Überwachung, Messung, Analyse und Bewertung

Der Umfang der Überwachungen und Messungen ist festgelegt und wird systematisch verfolgt. Die Informationssicherheitsleistung und die Wirksamkeit des Informationssicherheitsmanagementsystems werden laufend bewertet.

Dabei berücksichtigen wir:

- Was und wann überwacht und gemessen wird inklusive von Prozessen und Maßnahmen,
- Die Methodik,
- Die festgelegten Zyklen,
- Die Verantwortungen,
- Den Zeitpunkt und
- Wer die Ergebnisse analysiert und bewertet.

Das ISMS Team wertet die Ergebnisse aus und leitet bei Bedarf Korrekturmaßnahmen ein (Siehe auch Kapitel 10.2).

Prozess(e)
PA 9 1 0 Leistung Anbieter,
PA 7 5 3 Leistungsanalyse
Nachweis(e)
FB 9 1 0 Informationssicherheitsbericht
FB 9 1 0 Leistung Anbieter
FB 9 1 0 Leistungsbewertung
FB 9 1 0 Prüfplan

9 2 Internes Audit

9.2.1 Allgemeines

Interne Audits werden geplant und durchgeführt, um Informationen zu erhalten, ob:

- wir die Anforderungen an das Informationssicherheitsmanagementsystem erfüllen,
- die zugrundeliegende Norm eingehalten wird und
- das Informationssicherheitsmanagementsystem wirksam verwirklicht und aufrechterhalten wird.

Wir orientieren uns bei Audits an der DIN EN ISO 19011 Leitfaden für Audits von Qualitätsmanagement und/ oder Umweltmanagementsystemen sowie der ISO / IEC 27007 Auditrichtlinien.

Unsere Regelungen erfüllen:

- Planung,
- Aufbau,
- Aufrechterhaltung,
- Verwirklichung,
- Häufigkeit,
- Methoden,
- Verantwortlichkeiten,
- Planungsanforderungen und
- Berichterstattung
- von Auditprogrammen.

Sie berücksichtigen dabei:

- Qualitätsziele,
- Bedeutungen betroffener Prozesse,
- Rückmeldungen von Kunden,
- Änderungen mit Einfluss auf unser Unternehmen und
- die Ergebnisse vorheriger Audits.

Für Audits werden die Auditkriterien sowie der Umfang festlegt. Auditoren sind so ausgewählt, dass das Durchführen des Audits die Objektivität und Unparteilichkeit des Auditprozesses sichergestellt. Ergebnisse werden der zuständigen Leitung berichtet. Korrekturen und Korrekturmaßnahmen werden ohne ungerechtfertigte Verzögerungen umgesetzt. Dokumentierte Informationen werden bei den Unterlagen aufbewahrt.

9.2.2 Internes Auditprogramm

Wir betreiben ein Auditprogramm entsprechend der DIN EN ISO 19011. Wir dokumentieren die Audits und deren Ergebnisse.

Prozess(e)
PA 9 2 0 Internes Audit
Nachweis(e)
FB 9 2 0 Auditbericht,
FB 9 2 0 Auditcheckliste,
FB 9 2 0 Auditplan,
FB 9 2 0 Auditprogramm

9 3 Managementbewertung

9.3.1 Allgemeines

Wir analysieren und bewerten das ISMS mindestens jährlich auf seine Eignung, Angemessenheit und Wirksamkeit. Die Managementbewertung wird vom ISMS Team vorbereitet und von der obersten Leitung genehmigt.

9.3.2 Eingaben der Managementbewertung

Die Managementbewertung muss Folgendes umfassen:

a) Stand der Maßnahmen aus den letzten Bewertungen,
b) Veränderungen bei externen und internen Themen (Siehe 4.1 und 4.2),
c) Veränderungen in Bezug auf interessierte Parteien,
d) Ergebnisse und Trends zur ISMS-Leistung wie:
   1) Abweichungen und Korrekturmaßnahmen (Kapitel 10.2),
   2) Überwachungs- und Messergebnisse (Kapitel 9),
   3) Prüfungsergebnisse (Kapitel 8.1 und Kapitel 9),
   4) Erfüllung der Informationssicherheitsziele (Kapitel 6.2),
e) Ergebnisse aus Äußerungen von interessierten Parteien (Kapitel 9.1),
f) Ergebnisse der Risikobewertung und Status des Risikobehandlungsplans (Kapitel 8.2) und
g) Möglichkeiten zur kontinuierlichen Verbesserung (Kapitel 10.1).

9.3.3 Ergebnisse der Managementbewertung

Die Ergebnisse der Managementbewertung liefern Entscheidungen in Bezug auf die kontinuierlichen Verbesserungen und dem Änderungsbedarf am ISMS.

Nachweis(e)
FB 9 3 0 Managementbewertung

10 Verbesserung

10 1 Kontinuierliche Verbesserung

Wir verbessern laufend das ISMS durch Kontrollen und der Bewertung von Rückschlüssen. Verbesserungen werden in einem Maßnahmenplan gelenkt.

Nachweis(e)
FB 10 1 0 Maßnahmenplan,

10.2 Nichtkonformität und Korrekturmaßnahmen

Wenn wir nichtkonforme Prozessergebnisse erkennen, beachten wir folgendes:

- Wir reagieren umgehend und zeitnah,
- Maßnahmen werden beschlossen, kontrolliert und ggfs. korrigiert,
- Fehlerursachen analysieren um ein erneutes Auftreten zu minimieren,
- Systematische Überprüfung der Nichtkonformitäten,
- Ermittlung vergleichbarer Nichtkonformitäten,
- Dokumentation in einem Maßnahmenplan oder vergleichbarer Hilfsmittel,
- Die Bewertung der Ergebnisse.

Prozess(e)
PA 10 1 0 Korrekturmaßnahmen
PA 10 1 0 Nichtkonformitäten Dienstleistung

PA 10 1 0 Nichtkonformitäten Produkt
Nachweis(e)
FB 10 1 0 Maßnahmenplan,
FB 10 1 0 Fehlerliste,
FB 10 1 0 4D Report

11.0 Begriffserklärung (Grundlage ISO 27000)

Angriff

Der Versuch, Werte zu

- zerstören,
- offen zu legen,
- zu verändern,
- unbrauchbar zu machen,
- zu stehlen oder
- nicht autorisierten Zugriff erlangen sowie
- unberechtigte Nutzung

Zugriffskontrolle

Sicherstellung, dass der Zugriff auf Werte autorisiert und eingeschränkt erfolgt.

Zurechenbarkeit

Verantwortung für Handlungen und Entscheidungen.

Wert

Ist alles, was von Wert ist.

Authentisierung

Sicherstellung, dass behauptete Eigenschaften korrekt sind.

Authentizität

Eigenschaft die ist was sie zu sein vorgibt.

Business Continuity

Maßnahmen und Vorgaben, die der Sicherstellung eines kontinuierlichen Geschäftsbetriebs dienen.

Vertraulichkeit

Ausschluss der Verfügbarmachung und Enthüllung von Werten.

Maßnahme

Maßnahmen, Sicherheits- oder Gegenmaßnahmen zum Management von Risiken.

Korrekturmaßnahme

Ursachenbeseitigung von Fehlern oder unerwünschten Situationen.

Ereignis

Auftreten von außerordentlichen Umständen.

Richtlinie

Empfehlungen zur Zielerreichung.

Auswirkung

Verschlechterung des Niveaus erreichter Unternehmensziele.

Informationswert

Wertvolles Wissen oder Daten.

Informationssicherheit

Aufrechterhaltung

- Vertraulichkeit
- Integrität

- Verfügbarkeit
- Authentizität
- Zurechenbarkeit
- Nicht-Abstreitbarkeit
- und Verlässlichkeit

von Informationen.

Informationssicherheits-Ereignis

Erkennung von möglichen Verstößen gegen Leitlinien, Maßnahmenversagen und unbekannte Situationen sicherheitsrelevanten Charakter.

Informationssicherheits-Vorfall

Ein oder mehrere unerwartete Informationssicherheits-Ereignisse mit Bedrohungspotential.

Informationssicherheitsmanagementsystem (ISMS)

Teil des gesamten Managementsystems, das in Bezug auf die Informationssicherheit folgendes berücksichtigt:

- Entwicklung,
- Implementierung,
- Durchführung,
- Überwachung,
- Überprüfung,
- Instandhaltung und
- Verbesserung.

Informationssicherheits-Risiko

Die Möglichkeit Schaden zuzufügen.

Integrität

Absicherung von Richtigkeit und Vollständigkeit von Werten.

Leitlinie

Ausgedrückte Intention und Richtung.

Vorbeugungsmaßnahme

Maßnahme zur Ursachenbeseitigung möglicher Fehler oder unerwünschter Situationen.

Verfahren

Festgelegter Ablauf eine Tätigkeit oder einen Prozess durchzuführen.

Prozess

In Wechselbeziehung oder Wechselwirkung stehende Tätigkeiten zur Umwandlung von Eingaben in Ergebnisse.

Aufzeichnung

Dokument mit Nachweisen ausgeführter Tätigkeiten.

Verlässlichkeit

Eigenschaft der Übereinstimmung zwischen beabsichtigtem Verhalten und den Ergebnissen.

Risiko

Kombination aus Wahrscheinlichkeiten und deren Auswirkungen.

Risikoakzeptanz

Entscheidung, ein Risiko zu akzeptieren.

Risikoanalyse

Identifizierung von Risikoquellen zur Abschätzung des Risikos mit deren systematischen Gebrauch als Grundlage zur Risikobewertung, Risikobehandlung und Risikoakzeptanz.

Risikoeinschätzung

Kompletter Prozess der Risikoanalyse und Risikobewertung.

Risikokommunikation

Austausch und / oder Nutzung von Informationen über Risiken auf festgelegten Ebenen.

Risikokriterien

Rahmen zur Einschätzung eines Risikos.

Risikobestimmung

Wertzuordnung zur Wahrscheinlichkeit und den Auswirkungen eines Risikos.

Risikobewertung

Prozess, in dem eingeschätzte Risiken mit festgelegten Kriterien verglichen wird, um eine Bedeutung zu bestimmen.

Risikomanagement

Koordinierte Tätigkeit zur Leitung und Kontrolle einer Institution in Bezug auf Risiken mit:

- Risikoeinschätzung,
- Risikobehandlung,
- Risikoakzeptanz,
- Risikokommunikation,
- Risikoüberwachung und
- Risikoüberprüfung.

Risikobehandlung

Ablauf der Auswahl und Umsetzung von Maßnahmen zur Veränderung des Risikos.

Erklärung zur Anwendbarkeit

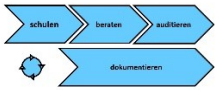
Dokument mit Beschreibung von Maßnahmenziele und Maßnahmen die anwendbar sind.

Bedrohung

Unter Möglichkeit stehender Anlass für ein unerwünschtes Ereignis.

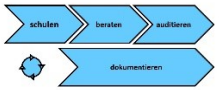
Schwachstelle

Schwäche eines Wertes oder einer Maßnahme die von anderen ausgenutzt werden kann.



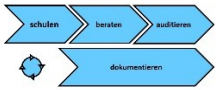
7.5.1 Dokumentierte Informationen

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	



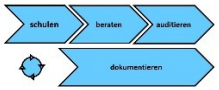
7.5.1 Dokumentierte Informationen

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	



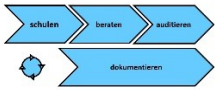
7.5.1 Dokumentierte Informationen

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 Informationssicherheitsrichtlinie	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	
6 1 2 / 6 1 3 Informationssicherheitsrisiko Beurteilung Behandlung	0		QM	QM	
6 1 3 Relevante Risiken	0		QM	QM	
6 2 0 Informationssicherheitsziele	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 Behandlungsplan ISMS Risiken	0		QM	QM	



7.5.1 Dokumentierte Informationen

Dokumentenübersicht	Revision	vom	Ersteller/-in	Verteiler	Grund der letzten Änderung
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	
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	



7.5.1 Dokumentierte Informationen

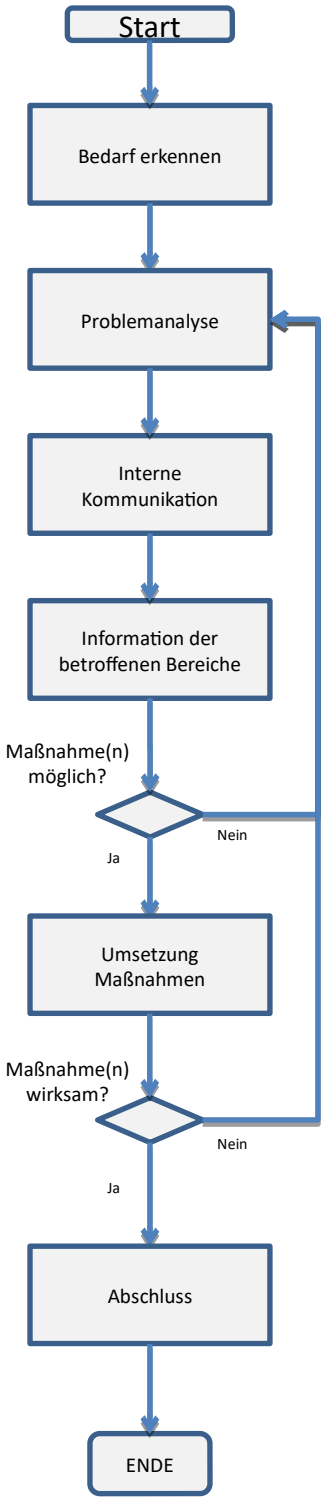
Dokumentenübersicht	Revision	vom	Ersteller/-in	Verteiler	Grund der letzten Änderung
8 3 0 Zugangssteuerung	0		QM	QM	
9 1 0 Informationssicherheitsbericht	0		QM	QM	
9 1 0 Leistung Anbieter	0		QM	QM	
9 1 0 Leistungsbewertung	0		QM	QM	
9 1 0 Prüfplan	0		QM	QM	
9 2 0 Auditbericht	0		QM	QM	
9 2 0 Auditcheckliste 27001	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 4D Report	0		QM	QM	
10 2 0 Liste Verbesserungen	0		QM	QM	

Liste geprüft und freigegeben:

Datum: Funktion, Unterschrift

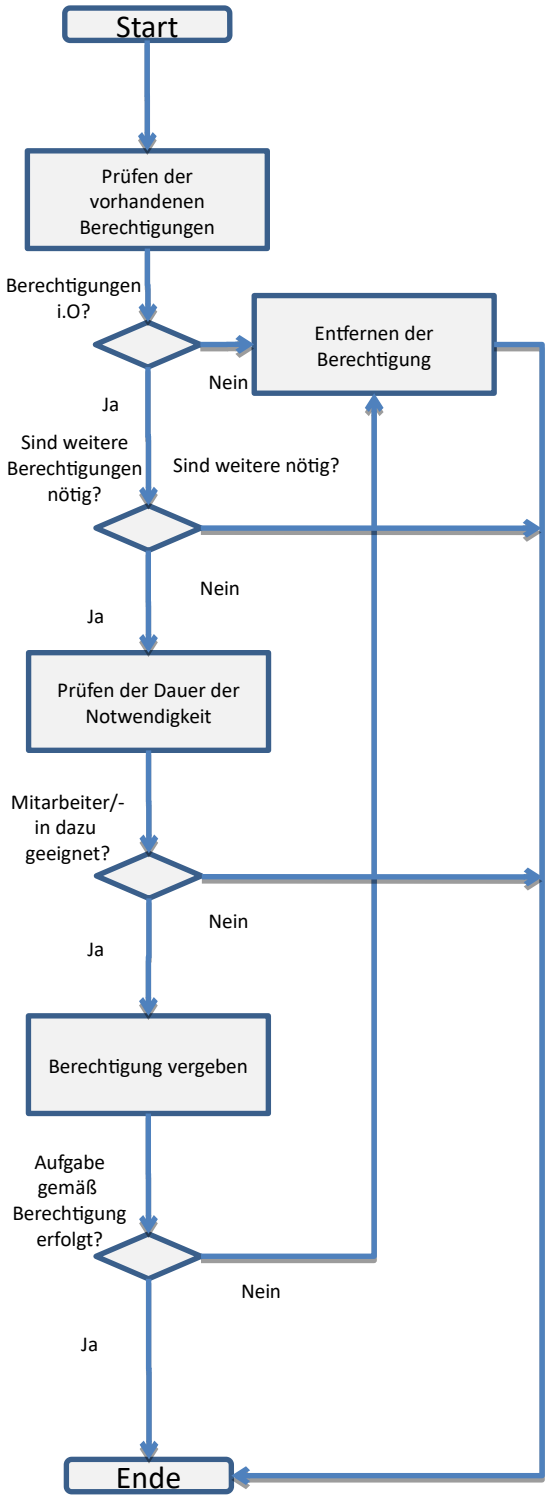
6.2.0 Planung Änderungen

MW	VA	Ablauf / Tätigkeiten	Dokumente	Ablauf / Hilfsmittel
	ISMS-Beauftr.	Bedarf erkennen	FB Änderungs-steuerung	Laufende Informationen aus dem ISMS wie Fehler, Korrekturen, Auswertungen, Leistungsbewertungen…
MA	ISMS-Beauftr.	Problemanalyse	FB Änderungs-steuerung	Bewertung der Ergebnisse im Hinblick auf notwendige Änderungen.
GF MA	ISMS-Beauftr.	Interne Kommunikation	FB Änderungs-steuerung	Besprechung des Problems und der möglichen Maßnahmen. Beurteilung des Handlungsbedarfs. Ableiten von Maßnahmen und Änderungen.
Bereiche	ISMS-Beauftr.	Information der betroffenen Bereiche	FB Änderungs-steuerung	Die betroffenen Bereiche (auch extern) werden in die Maßnahmen eingewiesen.
	ISMS-Beauftr.	Maßnahme(n) möglich? (Nein / Ja)	FB Änderungs-steuerung	Wirksam sind die Maßnahmen, wenn sie den gewünschten Erfolg bringen können. Verbesserungen werden vermerkt.
MA	ISMS-Beauftr.	Umsetzung Maßnahmen	FB Änderungs-steuerung	Das FB Änderungssteuerung beinhaltet alle Angaben zur Durchführung.
	ISMS-Beauftr.	Maßnahme(n) wirksam? (Nein / Ja)	FB Änderungs-steuerung	Die Maßnahme ist erfolgreich umgesetzt, wenn die Änderung wirksam geprüft wurde.
MA	ISMS-Beauftr.	Abschluss	FB Änderungs-steuerung , FB Management-bewertung	Abschließend: Informationen von betroffenen Bereichen und der GF über das Ergebnis. Die Ergebnisse gehen in die Managementbewertung ein.



MW = Mitwirkung
VA = Verantwortung

8.3.0 Berechtigung

MW	VA	Ablauf / Tätigkeiten	Dokumente	Ablauf Hilfsmittel
				
Ltg	ISMS-Beauftr.	Prüfen der vorhandenen Berechtigungen	Liste der Berechtigungen, Befugnismatrix	Die aktuellen Berechtigungen werden von der Leitung überprüft.
Ltg	ISMS-Beauftr.	Berechtigungen i.O?	Liste der Berechtigungen, Befugnismatrix	Sind die Berechtigungen nicht in Ordnung, werden diese abgeändert.
Ltg	ISMS-Beauftr.	Sind weitere Berechtigungen nötig?	Liste der Berechtigungen, Befugnismatrix	Sollten neue Berechtigungen notwendig sein, werden diese auf die Dauer der Notwendigkeit geprüft.
Ltg	ISMS-Beauftr.	Prüfen der Dauer der Notwendigkeit	Liste Berechtigungen, Befugnismatrix	
Ltg	ISMS-Beauftr.	Mitarbeiter/-in dazu geeignet?		Nach dem Ermitteln der Notwendigkeit der Dauer der Berechtigung wird geprüft, ob das Risiko der Vergabe der Berechtigung zu vertreten ist.
Ltg	ISMS-Beauftr.	Berechtigung vergeben	Liste der Berechtigungen, Befugnismatrix	Die Berechtigung wird vergeben und in die Liste der Berechtigungen eingetragen.
	ISMS-Beauftr.	Aufgabe gemäß Berechtigung erfolgt?	Liste der Berechtigungen, Befugnismatrix	Es werden die Aufgaben anhand der Berechtigung ermittelt und überprüft, sollte der Mitarbeiter diese nicht erfüllen, wird die Berechtigung entfernt.

MW = Mitwirkung
VA = Verantwortung

4.4.0 Prozesserstellung

Grundlagen

Kapitel 4 Abschnitt 4.4.0 "ISMS und dessen Prozesse“.

Gültigkeit

Diese Anweisung betrifft alle Personen, die Prozessbeschreibungen erstellen.

Ziel und Grund

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

Allgemeines

In unserem Unternehmen werden Prozessbeschreibungen nach vielfältiger Art erstellt. Um eine einheitliche Vorgehensweise zu gewährleisten, wurde diese Arbeitsanweisung erstellt.

Abkürzungen

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

Zu beachtende Punkte bei der Erstellung von Prozessbeschreibungen

In jeder Prozessbeschreibung beachten wir die folgenden Anforderungen:

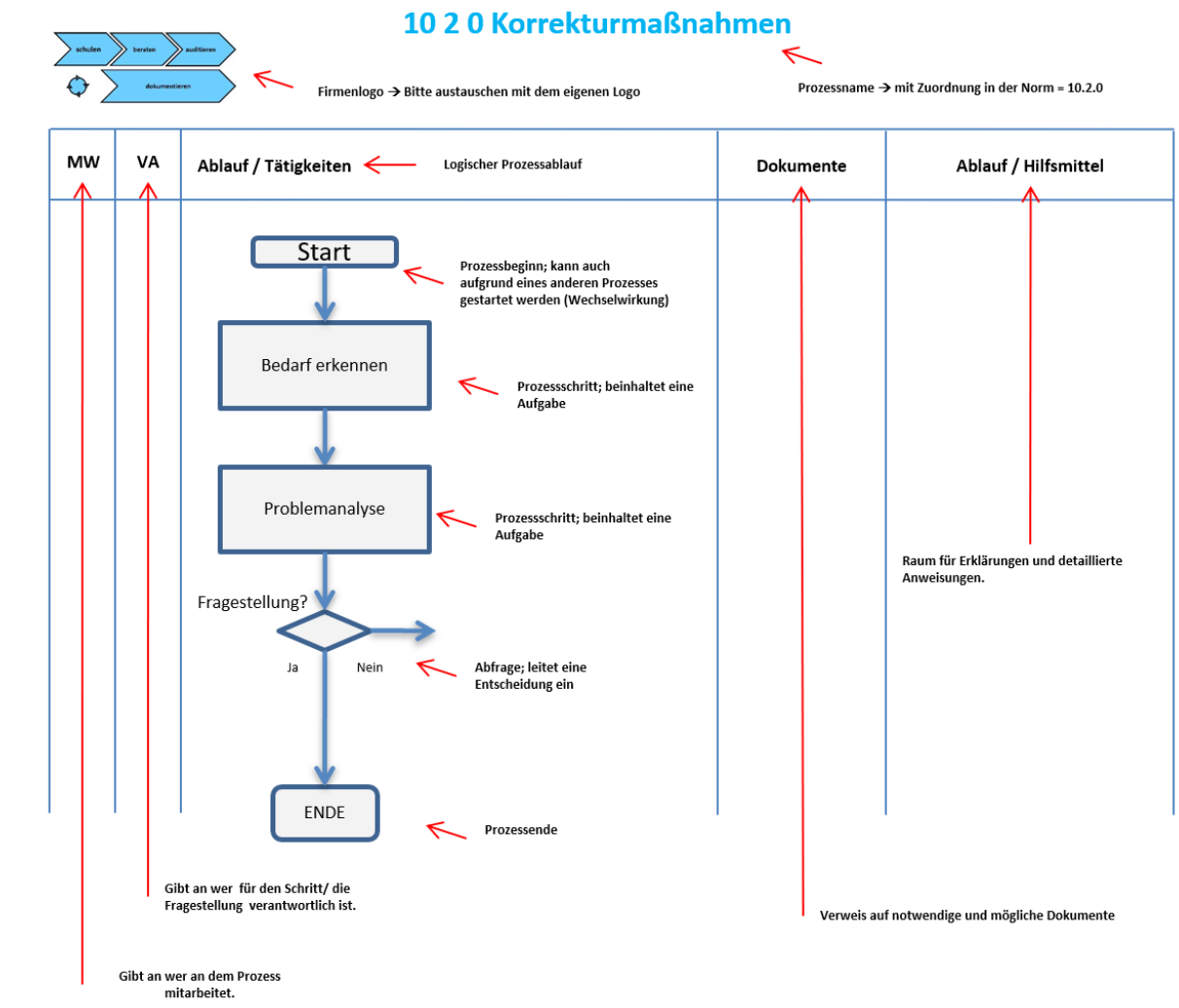
- Prozesseingaben
  - Die Eingaben, die für den Prozess notwendig sind. Beispiel: Lagerbestand, Materialeigenschaften für den Prozess Beschaffung.
- Prozessergebnis
  - Das Prozessergebnis, welches zu erwarten ist, muss festgelegt und dem Anwender bekannt gemacht sein. Beispiel: Weiterleitung der Unterlagen an die Verwaltung zur Bezahlung bei Beschaffungen.
- Kriterien und Methoden zur Durchführung
  - Die Kriterien zur Durchführung müssen hervorgehen. Beispiel: Zuwenig Produkte im Lager.

- Die Methode zur Durchführung ist festgelegt. Beispiel: Zählen des Bestandes und Suche nach Anbieter.

- Art der Messung
  - der Prozess kann gemessen werden. Manchmal macht es aber keinen Sinn, da der Prozess von geringer Bedeutung ist. Beispiel: Hat die Beschaffung stattgefunden.
- Messmethoden
  - Die Methode der Messung kann für jeden Prozess in der Beschreibung festgelegt werden oder global. Beispiel: Formblatt Leistungsanalyse.
- Leistungsindikatoren
  - Sie bestimmen die signifikanten Faktoren für die erfolgreiche Durchführung. Beispiel: Anbieter müssen geeignet sein.
- Verantwortungen / Befugnisse
  - Sie werden bei jeder Prozessbeschreibung genannt, um eindeutige Zuordnungen gewährleisten zu können. Beispiel: Verantwortung Beschaffung ist bei dem Einkauf, die Pflicht zur Mitarbeit haben die Bedarfsträger/-innen.
- Prozessrisiken, Chancen und abgeleitete Maßnahmen
  - Sie werden benannt und beachtet bei der Beschreibung des Prozesses. Sie müssen jedoch nicht zwingend im Prozess beschrieben sein. Beispiel: In der Beschaffung besteht das Risiko, das falsche Produkt zu beschaffen und die Chance, den Einkauf zu optimieren. Abgeleitete Maßnahmen sind nur bei freigegebenen Anbietern eine Beschaffung durchzuführen.
- Prozessüberwachung
  - Die Prozessüberwachung kann explizit festgelegt sein oder sie ergibt sich aus dem Prozess. Beispiel: Bestellungen werden vom System oder durch einen Ordner überwacht. Die Rechnung kommt jedoch stets von ganz allein.
- Änderungen
  - Prozessänderungen müssen beschrieben und dokumentiert sein, damit alle Beteiligten auch die Änderungen kennen. Beispiel: Die Verantwortung für die Beschaffung wechselt.
- Prozessverbesserungen
  - Prozessverbesserungen werden bei Erkennung einer Verbesserung durchgeführt, werden als Hinweis Dritter oder systematisch durch Auswertungen erkannt. Beispiel: Erweiterung der Einkaufsbedingungen.
- Dokumente und deren Aufbewahrung
  - Notwendige und festgelegte Dokumente / Informationen werden durch das QM-System gelenkt oder für den Prozess speziell festgelegt. Beispiel: Lieferscheine und Rechnungen werden vom Einkauf 10 Jahre aufbewahrt.
- Prozessabfolge und deren Wechselwirkungen
  - Bei jedem Prozess werden die logischen Abfolgen und Wechselwirkungen beschrieben. Beispiel: Fragestellungen in der Beschaffung.

4.4.0 Prozesserstellung

Grafisches Beispiel



8.3.0 Verwendung von Werten außerhalb des Unternehmens

Grundlagen

Kapitel 8 Abschnitt 8.3.0 " Informationsrisikobehandlung“.

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, Smartphones, Laptop, 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-Beauftragtem(n) gemeldet.

Qualitätsziele 20xx	Soll	Maßnahmen zur Erreichung	Verantwortlich	IST am:
ISMS-Ziele				
Ziel: Aufrechterhaltung der Informationssicherheit	100% Bereitschaft	Einführung ISMS im Unternehmen	ISMS-Beauftr.	
Ziel: Datenverlust durch Raub	Kein Verlust	Erstellen von Richtlinien um Datenverlust durch raub zu minimieren. Schützen der Verzeichnisse, Zutrittsregelungen	ISMS-Beauftr.	
Ziel: Datenverlust durch Ausfall	Kein Verlust	Zu c) laufende Wartung aller EDV-Einheiten und Überwachung der Funktion.	ISMS-Beauftr.	
Ziel: Datenverlust durch Sabotage	Kein Verlust	Zu d) Es wird ein redundantes System aufgebaut um Daten in jedem Fall beibehalten zu können. Es werden Regelungen auf allen Ebenen getroffen zum Umgang und Zugang zu Daten.		
Kundenzufriedenheit				
Ziel: Besuch der wichtigen Kunden	1x per anno	Besuchsplan erstellen.	Vertrieb	

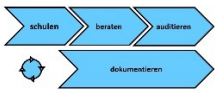
Qualitätsziele 20xx	Soll	Maßnahmen zur Erreichung	Verantwortlich	IST am:
Führung **Ziel: Einführung DIN EN ISO 9001 (Zertifizierung)**	100%	Aufbau Handbuch Zertifizierer vertraglich binden.	QM	
Mitarbeiter/-innenzufriedenheit **Ziel: Kündigungen wegen Unzufriedenheit**	0	Formlose Personalgespräche Halbjährlich. Liste erstellen.	GF	
Mitarbeiter/-innen **Ziel: Maschinenausfall wegen mangelnder Wartung**	0	Wartungsplan an jeder Maschine aushängen und überwachen.	Prod. Leitung	
Qualität Produkt **Ziel: Beanstandungen wegen Genauigkeit**	0	Prüfplan erstellen und überwachen.	QM, Ltg. Entwicklung, Ltg. Produktion	
Bereitstellung von Mitteln **Ziel: Planung eines Neubaus**	100%	Planungsbüro beauftragen und überwachen.	GF	

Qualitätsziele 20xx	Soll	Maßnahmen zur Erreichung	Verantwortlich	IST am:
Verbesserung der Prozesse **Ziel: Beschreibung der Prozesse im Rahmen des Qualitätsmanagementsystems**	Schulungskonzept Wartung	Schulungskonzept erstellen, prüfen und freigeben.	Ltg. Entwicklung, Vertrieb	
Anbieter von Lieferungen und Leistungen **Ziel: Bewertung der Anbieter**	1x komplett	Ermittlung der wichtigsten Anbieter	Einkauf	
Akquisition, Vertriebsziele **Ziel: Aufbau neuer Stammkunden**	> 1	Messebesuch in Saarbrücken	Vertrieb	
Vorkehrungen zum Schutz der Gesundheit und der Sicherheit am Arbeitsplatz **Ziel: Durchführung der Erst- und Folgeunterweisungen im Rahmen des Arbeitsschutzes.**	1x per anno	Externen Arbeitsschützer beauftragen	GF	
Umsetzung von Maßnahmen aus vorliegenden Bewertungen **Ziel: nicht belegbar**				
Ausschluss von Haftungsrisiken, Risikominimierung				

Qualitätsziele 20xx	Soll	Maßnahmen zur Erreichung	Verantwortlich	IST am:
Ziel: Ausführliche Einarbeitung von Auszubildenden und neuen Mitarbeiter/-innen	100%	Ausbilder beauftragen und Bericht anfordern	GF, Ausbilder	
Regulatorische Anforderungen **Ziel: Prüfung auf Neuerungen durch die Entwicklung**	2x per anno	Überwachung Internetseiten und Informationen der benannten Stelle	Qualitätsmanager/-in	
Technische Dokumentationen **Ziel: Prüfung der Produktakte auf Aktualität**	2x per anno	Prüfung halbjährlich und bei Anlässen wie Rückmeldungen, Fehler und vielem mehr.	Ltg. Entwicklung	

Freigegeben am: xx.xx.xxxx

Unterschrift GF, Datum



8.3.0 Konfiguration Medien **Beispiele in Rot**

Konfiguration Medien:

Gerät	Schutzart
Arbeitsrechner, Standard Konfiguration, MS Office	Passwortschutz für das Betriebssystem, Tägliche Kontrolle, USB-Ports gesichert
Laptops	
Server	
Mobilfunkgeräte	
Fahrzeuge	

Unbeaufsichtigte Benutzergeräte:

Gerät	Schutzart
Eingabeterminal Empfang	Passwortschutz für das Betriebssystem, tägliche Kontrolle, USB-Ports gesichert