Produktvorstellung

Qualitätsmanagement Verlag

Seiler Dokumentationen

Regelwerk Informationssicherheit nach DIN ISO/IEC 27001:2017 "neu" unter der "high level structure".

Egal was Du tust,
mach es mit Begeisterung!

MITGLIED IM DIN

Zielgruppe:

- **Unternehmen die ein Informationssicherheitsmanagementsystem betreiben wollen oder müssen. Dieses Handbuch ist für Unternehmen jeder Branche ausgelegt.**

Gliederung / Aufbau

- Regelwerk (10 Kapitel in einer Datei),
- Prozessbeschreibungen (52 Beispiele),
- Anweisungsbeispiele (8 Beispiele),
- Formblätter / Nachweisvorlagen (64 Beispiele)

Die Nummerierung entspricht der "high level structure" mit 10 Kapiteln. So kann eine Zuordnung zu anderen Normen leicht realisiert werden.

Lieferung

Per Download und oder Hardcover mit CD.

Leseprobe

Siehe Produktdatenblatt.

Allgemein

Das Thema Informationssicherheit ist in allen Unternehmen eine Frage. Bestimmte Unternehmen müssen ein System zur Informationssicherheit einführen. Da diese Unternehmen bereits eine Zertifizierung nach DIN EN ISO 9001 haben, haben wir die Anforderungen der DIN EN ISO 27001 in ein komplettes Regelwerk gepackt. In den Prozessbeschreibungen, Arbeitsanweisungen und Nachweisen wurden, wenn sinnvoll und notwendig, ergänzende Regelungen hinterlegt.

Grundlegende Änderungen zur zur Vorgängerversion haben wir in rot gekennzeichnet.

Der Aufwand zur Anpassung des Regelwerkes unter Beachtung von MS-Office Kenntnissen ist sehr gering. Für Unternehmen mit bestehender Zertifizierung, dient das Regelwerk für neue Ideen und der Findung von vollständigen und praktikablen Vorlagen.

Unterstützung bei der Umsetzung ist möglich.

Konditionen

Qualitätsmanagement Verlag

Seiler Dokumentationen

ISBN (Bei Bestellung über den Buchhandel):
ISBN 978-3-942882-67-5

Egal was Du tust,
mach es mit Begeisterung!

Mögliche Beratungsleistungen unter

www.erfolgsdorf.de

MITGLIED IM DIN

Lieferung
Lieferung als Hardcover mit CD oder
Download

Konditionen
- Keine Ergänzungslieferungen
- Rückgaberecht

Bestellung über den Buchhandel ist möglich.
In der Produktbeschreibung finden Sie die ISBN-Nummer.

Autor

Klaus Seiler, Master of science in quality management, berät Unternehmen bei der Einführung, Weiterentwicklung und Umsetzung von Managementsystemen.
Er ist Autor von zahlreichen Musterhandbüchern auf unterschiedlichen Normgrundlagen. Durch seine Erfahrungen als Berater, Sachverständiger, Lead- oder Zertifizierungs-Auditor kennt er die Probleme der Unternehmen bei der Umsetzung von Managementsystemen.
Die Musterdokumentationen sind das Ergebnis aus langjährigen Erfahrungen, der Lehre und aus Beratungen.

Microsoft® Office

Alle Dateien stehen
in MS-Office-Formaten zur Verfügung

Inhaltsverzeichnis

1 Anwendungsbereich 2
2 Normative Verweisungen 2
3 Begriffe (siehe Punkt 11) 2
4 Kontext der Organisation 2
4 1 Verstehen der Organisation und ihres Kontextes 2
4 2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien 2
4 3 Festlegen des Anwendungsbereichs des ISMS 3
4 4 ISMS 3
5 Führung 3
5 1 Führung und Verpflichtung 3
5 1 1 Führung und Verpflichtung 3
5 2 Politik 3
5 3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation 4
6 Planung 4
6 1 Maßnahmen zum Umgang mit Risiken und Chancen 4
6 2 Informationssicherheitsziele und Planung zu deren Erreichung 5
7 Unterstützung 5
7 1 Ressourcen 5
7 2 Kompetenz 5
7 3 Bewusstsein 6
7 4 Kommunikation 6
7 5 Dokumentierte Information 6
7 5 1 Allgemeines 6
7 5 2 Erstellen und Aktualisieren 6
7 5 3 Lenkung dokumentierter Informationen 7
8 Betrieb 7
8 1 Betriebliche Planung und Steuerung 7
8 2 Informationssicherheitsbeurteilung 7
8 3 Informationsrisikobehandlung 7
9 Bewertung der Leistung 8
9 1 Überwachung, Messung, Analyse und Bewertung 8
9 2 Internes Audit 8
9 3 Managementbewertung 9

Leseprobe

10 Verbesserung 9
10 1 Nichtkonformitäten und Korrekturmaßahmen 9
10 2 Fortlaufende Verbesserung 10
11.0 Begriffserklärung (Grundlage ISO 27000) 10

1 Anwendungsbereich

Unternehmensbezeichnung:	Mustermann AG
Straße:	Zum Saibling 3
PLZ, Ort:	D-88662 Überlingen
GF:	xy
ISMS-Beauftragte(r):	xy
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 27001:2017-03 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 27006:2017-01 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 ISMS

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 ISMS

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)

Qualitätsmanagement Verlag

Seiler

Dokumentationen

Informationssicherheitsmanagement

Prozessbeschreibungen

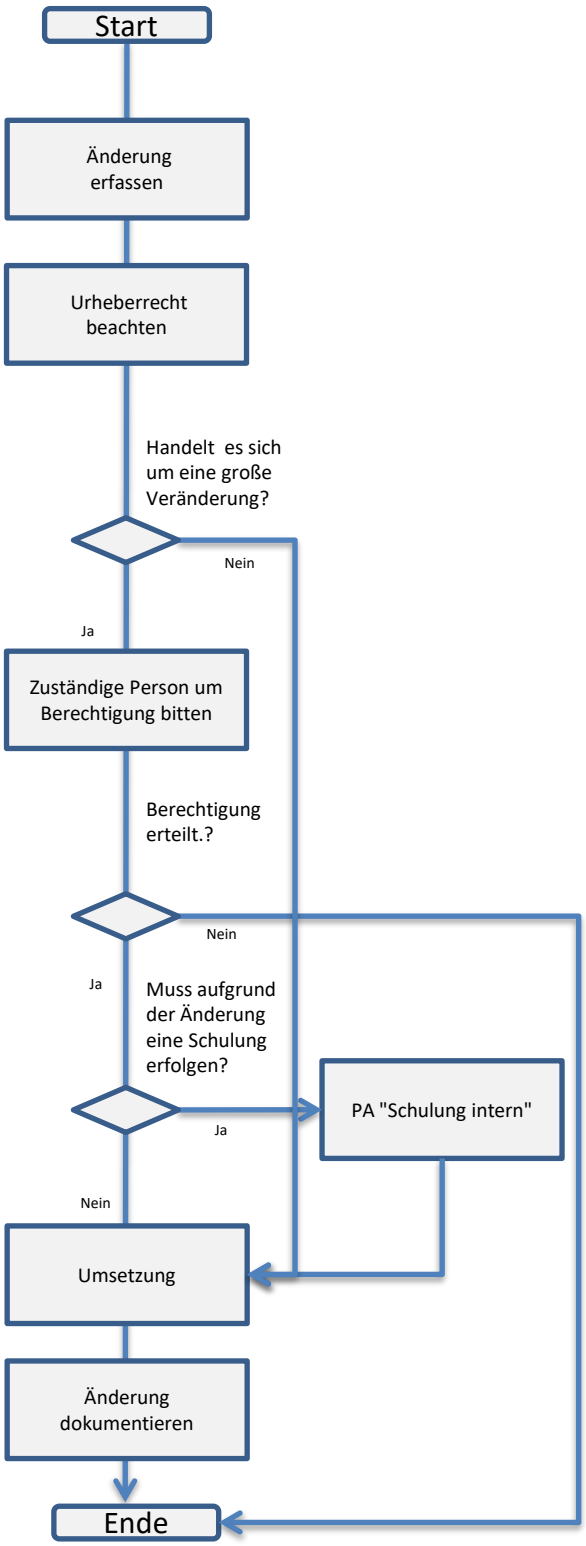
DIN EN ISO 27001:2017

Weitere Prozessbeschreibungen im Handbuch:

6 1 0 Ermittlung Risiken Chancen
6 1 2 Informationssicherheitsrisikobeurteilung
6 1 3 Informationssicherheitsbehandlung
6 1 3 Risikomanagement IT
6 2 0 Informationssicherheitsziele
6 3 0 Planung Änderungen
7 2 0 Erforderliche Kompetenzen
7 2 0 Schulungen
7 2 0 Weiterbildung
7 4 0 Externe Kommunikation
7 4 0 Interne Kommunikation
7 5 3 Lenkung aufgezeichneter Informationen
7 5 3 Lenkung externer Informationen
7 5 3 Lenkung interner Informationen
8 3 0 Änderungen am System
8 3 0 Auswahl Anbieter
8 3 0 Benutzerzugang
8 3 0 Berechtigung
8 3 0 Beschaffung
8 3 0 Eigentum Kunden Anbieter
8 3 0 Entsorgung Datenträger
8 3 0 Entwicklungsänderungen
8 3 0 Entwicklungsbewertung
8 3 0 Entwicklungseingaben
8 3 0 Entwicklungsergebnisse
8 3 0 Entwicklungsplanung
8 3 0 Entwicklungsvalidierung
8 3 0 Entwicklungsverifizierung
8 3 0 Externe Wartungen
8 3 0 Genehmigung neuer Einrichtungen
8 3 0 Informationsübertragung
8 3 0 Informationen
8 3 0 Installation
8 3 0 Interne Wartung
8 3 0 Kennzeichnung und Rückverfolgbarkeit
8 3 0 Kennzeichnung von Informationen
8 3 0 Kommunikation Anbieter
8 3 0 Kontrolle Lieferungen
8 3 0 Lieferanten / Anbieteraudit
8 3 0 Notfallvorsoge Management
8 3 0 Registrierung / Deregistrierung
8 3 0 Sammlung Beweismaterial
8 3 0 Sicherheitsvorfall
8 3 0 Validierung Software
8 3 0 Wechselmedien
9 1 0 Leistung Anbieter
9 1 0 Leistungsanalyse
9 2 0 Internes Audit
10 1 0 Nichtkonformitäten Dienstleistung
10 1 0 Nichtkonformitäten Produkt
10 2 0 Planung Verbesserung

8.3.0 Änderungen am System

MW	VA	Ablauf / Tätigkeiten	Dokumente	Ablauf Hilfsmittel
MA	ISMS-Beauftr.	Änderung erfassen	FB Änderungs-steuerung	Die notwendige Änderung an der informationsverarbeitenden Einrichtung oder am System wird erfasst und dokumentiert.
MA	ISMS-Beauftr.	Urheberrecht beachten	FB Änderungs-steuerung	Sofern ein Urheberrecht vorhanden ist, muss dieses beachtet werden. Lizenzvereinbarungen und Vorschriften müssen ebenfalls beachtet werden.
	ISMS-Beauftr.	Handelt es sich um eine große Veränderung? (Nein / Ja)		Prüfen, ob es sich dabei um eine große und relevante Veränderung handelt, wenn ja muss der / die ISMS-Beauftr. informiert werden und die Berechtigung zu Veränderung muss eingeholt werden. Ist es eine unwichtige Änderung wird der / die ISMS-Beauftr. informiert und die Änderung umgesetzt
MA	ISMS-Beauftr.	Zuständige Person um Berechtigung bitten	FB Änderungs-steuerung	
MA	ISMS-Beauftr.	Berechtigung erteilt.? (Nein / Ja)	FB Änderungs-steuerung	Sollte die Berechtigung nicht erteilt werden, wird der Vorgang in den Papierkorb verschoben. Bei Zustimmung wird der Schulungsbedarf ermittelt.
MA	ISMS-Beauftr.	Muss aufgrund der Änderung eine Schulung erfolgen? (Ja / Nein)		
		PA "Schulung intern"	PA Schulung intern	Einleitung und Durchführung einer Schulung gemäß PA Schulung.
MA	ISMS-Beauftr.	Umsetzung	FB Änderungs-steuerung	Die Änderung wird umgesetzt und entsprechend dokumentiert. Bei Änderungen am System sind Betriebsanweisungen und eventuelle Richtlinien zu beachten.
MA	ISMS-Beauftr.	Änderung dokumentieren	FB Änderungs-steuerung	Die Dokumentation zur Änderung wird in die Datensicherung aufgenommen.



MW = Mitwirkung
VA = Verantwortung

8.3.0 Informationen

MW	VA	Ablauf / Tätigkeiten	Dokumente	Ablauf Hilfsmittel
ISMS-Beauftr.	MA	Start Information erhalten	Information	Der Mitarbeiter erhält eine Information und prüft diese auf Relevanz.
	MA	Wichtige Information? Nein → Ende	Information	Die Information ist wichtig wenn sie für weiterführende Prozesse benötigt wird.
	ISMS-Beauftr.	Urheber-schutz? Ja → Berechtigung einholen	Information	Der Urheber der Information ist um Erlaubnis zu fragen und die Berechtigung wird mit der Information zusammen verarbeitet.
	MA	Nein → Information dokumentieren	Information	Ist die Information wichtig, wird sie dokumentiert.
	MA	Berechtigung zum Abspeichern vorhanden? Nein → Berechtigung einholen	Information	Für das Abspeichern der Information muss eventuell eine Berechtigung eingeholt werden, diese wird kurzzeitig erteilt um die Information bei dem vorgesehenen Datenträger / Verzeichnis abzulegen.
	ISMS-Beauftr.	Ja → Überprüfen der Daten	Information	Vor den Speichern werden die eingegebenen Daten erneut kontrolliert.
	ISMS-Beauftr.	abspeichern	Information	Die Information wird abgespeichert und eindeutig gekennzeichnet und sofern nötig mit einer Berechtigungssperre versehen. Bei der Weitergabe erfolgt eine Prüfung der Berechtigungen.
	ISMS-Beauftr.	Schulung notwendig? Ja → PA Schulung	Information, PA Schulung,	Müssen Personen bezüglich der neuen Information geschult werden, wird gemäß PA Schulung verfahren.
	ISMS-Beauftr.	Nein → Ablage Ende	Information	Die Ablage der Dokumente erfolgt in Beweisqualität und wird entsprechend den Richtlinien aufbewahrt (min. 10 Jahre).

MW = Mitwirkung
VA = Verantwortung

Qualitätsmanagement Verlag

Seiler Dokumentationen

Informationssicherheitsmanagement

Arbeitsanweisungen

DIN EN ISO 27001:2017

Weitere Arbeitsanweisungen im Handbuch:

- 4 4 0 Anweisung Prozesserstellung
- 8 3 0 Arbeiten in Sicherheitsbereichen
- 8 3 0 Entwicklungssteuerung
- 8 3 0 Kennzeichnung Informationen
- 8 3 0 Kontrolle Bereitstellungen
- 8 3 0 Transaktionen bei Anwendungsdiensten
- 8 3 0 Verwendung von Werten außerhalb des Unternehmens

Grundlagen 1
Gültigkeit 1
Ziel und Grund 1
Abkürzungen 1
Zu beachtende Punkte bei der Kontrolle von Bereitstellungen 1
Allgemeines 1
Forderungen 1
Zu den Unterpunkten: 2
Prüfungsmatrix 4
Steuerung der Dienstleistungserbringung von Lieferanten 5

Grundlagen

Kapitel 8 Abschnitt 8.3.0 " Informationsrisikobehandlung“.

Gültigkeit

Diese Anweisung betrifft alle Personen, die Bereitstellungen prüfen.

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 bei der Kontrolle von Bereitstellungen

Allgemeines

Die Firma MS-Seiler legt anhand des Ergebnisses der Lieferantenbewertung und der Bedeutung der Ware den Prüfumfang fest. Durch eine systematische Wareneingangsprüfung wird sichergestellt, dass fehlerhaftes Material und fehlerhafte Teile erkannt, gekennzeichnet und aussortiert werden.

Forderungen

Zur Einlagerung oder Freigabe gelangt nur geprüftes Material oder geprüfte Teile. Bei Lieferanten, bei denen im Laufe eines Kalenderjahres keine Beanstandungen aufgetreten sind, kann auf verschie-

dene Prüfungen verzichtet werden. Die Durchführung der Prüfung wird auf dem Lieferschein durch einen Zahlencode (Beispiel: 13042010LS oder 13.04.10 KS) des Ausführenden bestätigt. Bei Beanstandungen erstellt der Prüfer einen 4D-Report und übergibt diesen der Ltg. Einkauf zur Reklamation. Beanstandete Ware wird mit einem Sperrvermerk versehen und verbleibt bis zur Entscheidung über die weitere Vorgehensweise im Sperrlager.

Beim Wareneingang werden folgende Unterpunkte beachtet:

- Vollständigkeit
- Identität
- Beschaffenheit
- Prüfung der Lieferpapiere
- Optische Prüfung der Ware
- Abstellen der Ware
- Abstellplatz
- Lager
- Bestellnummer
- Menge
- Witterung
- Gebinde
- Beschädigung
- Palette
- Zertifikat
- Lieferschein
- Anlieferung
- Termin
- Kennzeichnung der Ware
- Konservierung
- Fehlerfall

Zu den Unterpunkten:

- Prüfung der Lieferpapiere

Vor dem Ausladen der Ware ist festzustellen, ob die Ware bestellt und eine Überlieferung von 10 % nicht überschritten wurde. Ebenfalls darf es nicht zu einer Unterlieferung von 10 % kommen.

- Optische Prüfung der Ware

Sind die Lieferpapiere in Ordnung, wird die Ware ausgeladen und einer optischen Prüfung unterzogen. Ist die Verpackung der Ware oder die Ware selbst in irgendeiner direkt erkennbaren Form beschädigt, wird dies auf den Lieferpapieren der Spedition handschriftlich vermerkt. Ist ein erheblicher Schaden zu erkennen, welcher den Einsatz der Ware in Frage stellt, wird die Ltg. Einkauf sofort telefonisch informiert und die weitere Vorgehensweise besprochen. Der Bestellende der Ware ist durch die Bestellnummer zu erkennen.

- Abstellen der Ware “Wareneingang”

Ist die Ware scheinbar in Ordnung, ist sie an dem für Wareneingang gekennzeichneten Platz abzustellen und die Lieferpapiere des Lieferanten sind zu unterzeichnen. Am Wareneingang darf die Ware nicht länger als 3 Tage stehen und muss schnellstmöglich überprüft werden.

- Abstellplatz im Aussenbereich

Es ist ein möglichst trockener Platz zu wählen. Falls das Gebinde der Witterung nicht ausgesetzt werden darf, wird unverzüglich die Ware an einem geeigneten Ort abgestellt, bzw. die Ltg. Produktion informiert.

- Lager

Die eingehende Ware ist im Lager an dem dafür vorgesehenen Lagerplatz abzustellen.

- Bestellnummer

Die Ware wird auf die Richtigkeit der Bestellung, bzw. Bestellnummer überprüft.

- Menge

Bei geschlossenen Gebinden wird entweder ein Rütteltest oder ein Sichttest auf Menge durchgeführt. Für alle anderen Produkte wird ein Zählverfahren angewendet. Ist das Gebinde bezüglich der Menge glaubhaft (2 Paletten, etc.) kann auf eine Wiegung, bzw. Zählung verzichtet werden.

- Witterung

Anfällige, bzw. empfindliche Ware darf nicht im Außenbereich abgestellt werden. Falls die räumliche Situation dies nicht zulässt, wird eine dafür vorgesehene Plane verwendet.

- Gebinde

Die Gebinde müssen in einwandfreiem Zustand sein. Da eventuelle Umweltemissionen zu größeren Schäden führen können, ist in diesem Falle die Lieferung immer abzulehnen.

- Beschädigung

Ist die Ware offensichtlich beschädigt, kann wie folgt verfahren werden:

- Die Lieferung kann nicht mehr abgelehnt werden → 4D-Report erstellen und Lieferung im Sperrlagerbereich abstellen, Lieferung kennzeichnen, Ltg. Einkauf verständigen.
- Die Lieferung kann noch abgelehnt werden → auf dem Lieferschein "Annahme verweigert“ mit kurzen Begründung vermerken, Unterschrift und Datum angeben, Ltg. Einkauf verständigen.
- Die Lieferung ist teilweise beschädigt → auf dem Lieferschein „Annahme unter Vorbehalt“ vermerken, die beschädigte Ware wird auf dem Lieferschein in Menge festgehalten, die Ware wird entsprechend gekennzeichnet und im Sperrlagerbereich (schadhafte Ware) oder dem Lager (verwendbare Ware) abgestellt. Unterschrift und Datum angeben. Ltg. Einkauf verständigen.

- Palette

Die Palette ist, wenn möglich, dem Spediteur zu übergeben. Es kann auch eine Ersatzpalette herangezogen werden. Weist der Lieferschein eine Belastung unseres Unternehmens an Paletten auf, so wird versucht, einen entsprechenden Ersatz zu übergeben. Der Ersatz wird auf dem Lieferschein vermerkt.

- Zertifikat

Zertifikate werden eingezogen und mit dem Lieferschein der Verwaltung übergeben. Ist die Ware zertifikatspflichtig, wird das Fehlen auf dem Lieferschein vermerkt.

- Lieferschein

Grundsätzlich gilt die Regel "Keine Annahme ohne Lieferschein oder ähnliches Dokument“. Ist ein Lieferschein dennoch nicht vorhanden, kann ein eigener Lieferschein erstellt werden.

Der Lieferschein beinhaltet:

- Ort
- Datum
- Anliefernder
- Annehmender
- Ware (Bezeichnung)
- Menge
- Zustand
- Paletten
- Zertifikate
- Ggf. weitere Informationen
- Termin

Weicht die Lieferung vom geforderten Termin ab, wird dies auf dem Lieferschein vermerkt, da es hier zu Abschlägen bei der Rechnung kommen kann.

- Kennzeichnung der Ware

Es ist wie folgt zu verfahren:

- Die Ware ist verwendungsfähig → ist die Ware noch nicht gekennzeichnet, wird sie mit einem entsprechenden Aufkleber versehen und an den dafür vorgesehenen Ort abgestellt.
- Die Ware ist nicht verwendungsfähig → die Ware wird entsprechend gekennzeichnet und im Sperrlagerbereich (schadhafte Ware) abgestellt, die Ltg. Einkauf wird verständigt.
- Die Ware ist teilweise beschädigt → die Ware wird entsprechend gekennzeichnet und im Sperrlagerbereich (schadhafte Ware) oder dem Lager (verwendbare Ware) abgestellt, die Ltg. Einkauf wird verständigt.

- Konservierung

Kann die Haltbarkeit des Produktes durch Konservierung weiter verbessert werden, wird die Ltg. Einkauf über diese Möglichkeit informiert. Die Ltg. Einkauf leitet die weiteren Maßnahmen ein.

- Fehlerfall

Grundsätzlich werden Abweichungen der Ltg. Einkauf mitgeteilt. Es ist jedoch nach dem Grundsatz "Die Erhaltung der Ware steht im Vordergrund“ zu verfahren.

Prüfungsmatrix

Prüfpunkt / Artikel	Flüssigstoffe	Feste Stoffe
Verpackung	X	X
Inhalt	X	
Beschädigung		X
Menge	X	X
Gebinde	X	
Zertifikat	X	
Termin	X	X

Steuerung der Dienstleistungserbringung von Lieferanten

Lieferantenleistungen auf dem Betriebsgelände werden laufend überwacht. Alle „digitalen Dienstleistungen“ werden vom / von der ISMS-Beauftragten überwacht.

Lieferantenleistungen werden zu 100% überwacht. Das Angebot wird Stück für Stück abgehakt. Installierte Programme werden auf Funktion geprüft.

Alle Lieferantenleistungen werden in der Datei „Informationssicherheitsrisiko Beurteílung Behandlung“ beachtet und bewertet. Bei Änderungen werden die Risiken erneut bewertet.

Qualitätsmanagement Verlag

Seiler

Dokumentationen

Informationssicherheitsmanagement

Formblätter / Nachweise

DIN EN ISO 27001:2017

Weitere Formblätter / Nachweise im Handbuch:

4 1 0 Kontext, Erfordernisse und Erwartungen
4 4 0 Grundriss Räumlichkeiten
4 4 0 Prozesse
5 2 0 Informationssicherheitspolitik
5 2 0 Informationssicherheitsrichtlinie
5 2 0 Lieferantensicherheitsrichtlinie
5 3 0 Organisationsdiagramm
5 3 0 Verantwortungen und Befugnisse
6 1 0 Chancen und Risiken
7 1 0 Werte
7 2 0 Benennung ISMS Beauftragte
7 2 0 Kompetenzen
7 2 0 Schulungsplan
7 4 0 Liste Kommunikationswege
7 4 0 Protokoll Besprechung
7 5 1 Dokumentierte Informationen (diese Liste)
8 1 0 Planung und Steuerung
8 2 0 Informationssicherheitsbeurteilung
8 3 0 Abnahmetest Software
8 3 0 Änderungssteuerung
8 3 0 Aktionsplan baulich organisatorisch
8 3 0 Ausgabe Mobilgeräte
8 3 0 Ausgabeliste Schlüssel
8 3 0 Berechtigungen
8 3 0 Entsorgungsprotokoll Wiederverwendung
8 3 0 Entwicklungsänderungen
8 3 0 Geheime Authentifizierungsinformationen
8 3 0 Information Arbeitsumgebung
8 3 0 Infrastruktur Netzwerkplan
10 1 0 8 D Report
10 2 0 Liste Verbesserungen
8 3 0 Kapazitätssteuerung
8 3 0 Kennwortsystem
8 3 0 Kennzeichnung / Rückverfolgung
8 3 0 Konfiguration Medien
8 3 0 Liste Anbieter
8 3 0 Liste bindende Vorgaben
8 3 0 Liste der Berechtigungen
8 3 0 Maßnahmen Wartung
8 3 0 Notfallplan
8 3 0 Protokollierung Überwachung
8 3 0 Prüfplan
8 3 0 QSV Qualitätssicherungsvereinbarung
8 3 0 Regelwerk Zugangskontrolle
8 3 0 Schweigepflicht externe Anbieter
8 3 0 Schweigepflicht Verantwortungsbelehrung
8 3 0 Sicherheitseinstufungen
8 3 0 Tätigkeiten Installation
8 3 0 Überwachung Änderungen
8 3 0 Unterschriftenliste
8 3 0 Zugangssteuerung
9 1 0 Informationssicherheitsbericht
9 1 0 Leistung Anbieter
9 1 0 Leistungsbewertung
9 2 0 Auditbericht
9 2 0 Auditcheckliste 27001 2017
9 2 0 Auditplan
9 2 0 Auditprogramm
9 3 0 Managementbewertung
10 1 0 Fehlerliste
10 1 0 Maßnahmenplan

ISMS:

- Anforderungen:
  - Aufrechterhaltung der Informationssicherheit
  - Datenverlust durch Raub
  - Datenverlust durch Ausfall
  - Datenverlust durch Sabotage
- Prozesskriterien für die Annahme:
  - Die Ziele müssen eingehalten werden
  - Es darf keinen Datenverlust geben.
- Ressourcen:
  - Infrastruktur
  - ISMS Beauftragte
- Prozessteuerung:
  - Laufende Überwachung von Ergebnissen
  - Beherrschung Notfälle
- Dokumentierte Informationen:
  - Alle Prozessbeschreibungen, Anweisungen und Erklärungen

Die Beschreibung ist ausreichend zur Aufrechterhaltung des Informationssicherheitsmanagementsystems.

8.3.0 Kapazitätssteuerung

Beispiele in Rot

Kapazität	Derzeitiger Einsatz	Standort	Auslastung in %	Redundanz	Erweiterung?
Raum	Serverraum mit Installation und Klimaanlage	UG 1, Raum 025	70	Nebenraum	Nicht vor 90% Auslas-tung
Mobile Geräte					
Personal					
Rechner					