[Logo der Organisation]

[Name der Organisation]

Commented [27A1]: Alle mit eckigen Klammern [ ] markierten Felder in diesem Dokument müssen ausgefüllt werden.

VERFAHREN ZUR IDENTIFIKATION DER ANFORDERUNGEN

Code:	
Version:	
Datum der Version:	
Erstellt durch:	
Genehmigt durch:	
Vertraulichkeitsstufe:	

Commented [27A2]: Die Systematik für die Kodierung von Dokumenten sollte dem in der Organisation vorhandenen System zur Dokumentations-Kodierung entsprechen. Falls kein solches System vorhanden ist, kann diese Zeile gelöscht werden.

Änderungs-Historie

Datum	Version	Erstellt durch	Beschreibung der Änderung
	0.1	27001Academy	Erster Entwurf des Dokuments

Inhaltsverzeichnis

1. Zweck, Anwendungsbereich und Anwender

Der Zweck dieses Dokuments ist die Beschreibung des Verfahrens zur Identifikation der Interessierte Parteien sowie der rechtlichen, amtlichen, vertraglichen und anderen Anforderungen mit Bezug zu Informationssicherheit. Ebenso werden darin die Verantwortlichkeiten für die Erfüllung dieser Anforderungen beschrieben.

Dieses Dokument wird auf das gesamte Informationssicherheits-Managementsystem (ISMS) angewendet.

Anwender dieses Dokuments sind alle Mitarbeiter von [Name der Organisation].

Commented [27A3]: Geben Sie bitte den Namen Ihrer Organisation an.

2. Referenzdokumente

- ISO/IEC 27001 Norm, Abschnitt 4.2, Maßnahme A.18.1.1
- Informationssicherheitspolitik

3. Identifikation der Anforderungen und interessierten Parteien

[redacted] ist verantwortlich für die Identifikation (1) aller Personen oder Organisationen, die von Informationssicherheit oder betrieblichem Kontinuitätsmanagement betroffen sein könnten oder darauf Einfluss haben könnten (interessierte Parteien) und (2) aller relevanten rechtlichen, amtlichen, vertraglichen oder anderen Anforderungen.

[redacted] legt fest, wer für die Einhaltung jeder einzelnen Anforderung verantwortlich ist und welche interessierte Parteien im Falle von Änderungen in Kenntnis gesetzt werden müssen.

[redacted] muss alle Anforderungen, interessierte Parteien und Verantwortlichen in der „Liste rechtlicher, amtlicher, vertraglicher und anderer Anforderungen“ aufführen und diese Liste im [Ortsangabe] veröffentlichen.

Jeder Mitarbeiter von [redacted] muss [redacted] benachrichtigen, falls er/sie von irgendeiner neuen rechtlichen, amtlichen, vertraglichen oder anderen Anforderung Kenntnis erlangt, die für Informationssicherheit und betriebliches Kontinuitätsmanagement relevant sein könnte.

Commented [27A4]: Dieser Artikel wird Ihnen helfen, Anforderungen zu identifizieren:

How to identify ISMS requirements of interested parties in ISO 27001 https://advisera.com/27001academy/blog/2017/02/06/how-to-identify-isms-requirements-of-interested-parties-in-iso-27001/

Commented [27A5]: Dieser Artikel hilft Ihnen, die Interessierte Parteien zu identifizieren:

How to identify interested parties according to ISO 27001 and ISO 22301 https://advisera.com/27001academy/knowledgebase/how-to-identify-interested-parties-according-to-iso-27001-and-iso-22301/

Commented [27A6]: ZB Sicherheitsmanager, Informationssicherheitsmanager usw.

Commented [27A7]: ZB Sicherheitsmanager, [redacted]

Commented [27A8]: ZB Sicherheitsmanager, Informationssicherheitsmanager usw.

Commented [27A9]: Beschreibung, wie und wo die Liste [redacted]

Commented [27A10]: Geben Sie bitte den Namen Ihrer Organisation an.

Commented [27A11]: Zum Beispiel: Sicherheitsmanager, [redacted]

4. Überprüfung und Bewertung

[redacted] ist dafür verantwortlich, dass die Liste der rechtlichen, gesetzlichen, vertraglichen und anderen Anforderungen mindestens [redacted] überprüft und bei Bedarf aktualisiert wird. [redacted] wird alle relevanten interessierte Parteien über jede Aktualisierung informieren.

Commented [27A12]: ZB Informationssicherheitsmanager, Prozessverantwortlicher, Verantwortlicher Geschäftsbereich usw.

Commented [27A13]: Nach Bedarf ändern.

Commented [27A14]: ZB Sicherheitsmanager, [redacted]

[redacted] mindestens einmal jährlich durchgeführt.

Commented [27A15]: ZB Sicherheitsmanager, [redacted]

Commented [27A16]: Zur Vereinfachung des Vorgangs kann dies auch vom internen Auditor erledigt werden.

Commented [27A17]: Nach Bedarf ändern.

5. Verwaltung der auf der Basis dieses Dokuments aufbewahrten Aufzeichnungen

Name der Aufzeichnung	Aufbewahrungsort	Für die Aufbewahrung verantwortliche Person	Maßnahme für Aufzeichnungsschutz	Aufbewahrungszeit
Liste rechtlicher, amtlicher, vertraglicher und anderer Anforderungen (in elektronischer Form)	Betriebliches Intranet	[Stellenbezeichnung]	Nur falls [Stellenbezeichnung] zur Bearbeitung von Daten berechtigt ist	Alte Versionen der Liste werden 3 Jahre lang archiviert

Commented [27A19]: Zum Beispiel: Sicherheitsmanager, Informationssicherheitsmanager, Compliance-Beauftragter usw.

Commented [27A18]: Nach Bedarf ändern.

Commented [27A20]: Zum Beispiel: Sicherheitsmanager, Informationssicherheitsmanager, Compliance-Beauftragter usw.

6. Gültigkeit und Dokumenten- Handhabung

Dieses Dokument ist gültig ab [Datum].

Der Eigentümer des Dokuments ist [Stellenbezeichnung], der das Dokument mindestens einmal jährlich prüfen und gegebenenfalls aktualisieren muss.

Commented [27A21]: Zum Beispiel: Sicherheitsmanager, Informationssicherheitsmanager, Compliance-Beauftragter usw.

Für die Auswertung des Dokuments auf Wirksamkeit und Angemessenheit müssen folgende Kriterien berücksichtigt werden:

- [redacted]
- [redacted]
- [redacted]

7. Anhänge

- Anhang 1 – Liste gesetzlicher, amtlicher, vertraglicher und anderer Anforderungen

[Stellenbezeichnung]
[Name]

_____

[Unterschrift]

Commented [27A22]: Nur notwendig, falls das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen das Unterschreiben von Papierdokumenten vorschreibt.